

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

零基础入门 快速掌握软件应用



SO EASY TO LEARN!!

黑客攻防

从新手到高手

蒋媛媛 编著



精选50个精彩视频直播

6小时案例讲解全程再现

附赠《电脑常见故障诊断与排除从新手到高手》和《系统优化与故障排除从新手到高手》教学视频

- 采用全程图解的形式编写 可操作性强 立竿见影
- “全程图解教学+多媒体视频讲解”教学模式 轻松上手
- 超值光盘互动教学 书盘完美结合

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防

从新手到高手



超值附赠

《电脑常见故障诊断与排除从新手到高手》



300分钟
多媒体教学演示

《系统优化与故障排除从新手到高手》

360分钟
多媒体教学演示



多媒体视频光盘



视频教学演示：



视频案例演示：



多媒体教学：

- 13个专题细致讲解，深入剖析
- 360分钟多媒体视频演示，轻松学习
- 大量精彩实例完美讲解，边学边练

制胜法宝1

图解互动全新教学法+
轻松攻克难关的视频教学



制胜法宝2

个性化情景写作方法+
技巧说明的新手学习模式



制胜法宝3

轻松的分步骤分解剖析+
自学不求人的掌上宝手册

责任编辑：苏茜 封面设计：张丽 封面制作：白雪 上架建议：计算机/网络技术/网络安全



中国铁道出版社 计算机图书批销部
地址：北京市宣武区右安门西街8号
邮编：100054

网址：<http://www.tqbooks.net>
读者热线电话：(010) 63560056
销售服务电话：(010) 83550290/91 83550580

ISBN 978-7-113-11246-2



9 787113 112462 >

ISBN 978-7-113-11246-2

定价：39.80 元（附赠光盘）

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防从新手到高手

Foreword

前言

编写简介

目前，互联网在不断地迅猛发展，给人们的生活提供了无限自由和大量财富，也为广大网民间的交流提供了极大方便。但是，与此同时互联网也带来了消极影响，“信息垃圾”、“邮件炸弹”、“电脑病毒”、“黑客入侵”等越来越威胁到网络的安全。尤其是电脑黑客攻击，现在已成为威胁网络安全的最大隐患。

本书旨在使读者了解黑客的攻击手段，使读者在实际网络应用中遇到黑客攻击时，能够最大限度地减少损害和损失。更为重要的是，希望读者能够运用本书介绍的攻防技术来防范黑客的恶意攻击，使自己的网络更加安全。

内容概述

本书的主线是电脑黑客的“攻”与“防”，每章基本上都是围绕这两点进行深入讲解的。内容涵盖黑客攻防工具和各种黑客攻防技术，并着重讲解了电脑安全软件的使用以及黑客攻防实战技巧等实用知识。

全书共分为 13 章，主要内容包括黑客基础知识、常用扫描与嗅探工具、Windows 系统漏洞攻防、设置系统安全策略、系统与文件加密、远程控制攻防、木马攻防、聊天软件攻防、网页恶意代码攻防、电子邮件攻防、U 盘病毒攻防、使用电脑安全软件、黑客攻防实用技巧等知识。

本书特色

每个初学者都想通过最行之有效的学习方法、最简洁易懂的讲解方式尽可能多地掌握电脑操作技能和技巧，本书将是您最好的选择。本书由资深电脑教育专家精心策划编写而成，主要具有以下特色：

内容全面权威、讲解深入浅出：针对电脑初学者，内容涵盖电脑黑客攻防的各个方面，权威全面、循序渐进，讲解清晰明了、深入浅出，让读者一看就懂，一练就会。

全程实战图解、注重学习方法：采用全程图解的形式组织编写，简便直观、可操作性强，并注重培养读者正确、高效的学习方法，达到立竿见影的学习效果。

全新教学模式、提升实战技能：采用“全程图解教学+多媒体视频讲解”的模式，并以图解标注出讲解关键性操作步骤，使读者轻松掌握实战操作技能，即学即用。

光盘互动教学、书盘完美合一：超长全新的多媒体互动学习光盘，囊括全书重要知识点和所有实战操作的全程教学视频或课件，为读者提供了一套生动鲜明的“活教材”。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

适用读者

本书适用面广，主要适合以下读者群体学习使用：

- （1）没有任何电脑黑客攻防知识的初学者；
- （2）对电脑黑客攻防技术有些了解但不精通的学习者；
- （3）网络安全从业人员以及网络管理员；
- （4）大中专院校的在校学生和社会电脑安全培训机构的学员；
- （5）想在短时间内全面掌握电脑安全实用技能的读者朋友。

售后说明

如果读者在使用本书的过程中遇到什么问题或者有什么好的意见或建议，可以通过发送电子邮件（E-mail: jtbook@yahoo.cn）或者在线（QQ: 843688388）联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

希望本书能对广大读者朋友提高学习和工作效率有所帮助，由于编者水平有限，书中可能存在不足之处，欢迎读者朋友提出宝贵意见，我们将加以改进，在此深表谢意！

特别提醒

根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术攻击他人电脑，否则后果自负，特此声明！

编 者
2010 年 3 月

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客精神：

技術共享，資源共享，資料共享

**不求最好，只求較好
做中國較好的網絡安全資料站**

**300G成套精品教程免费下载
每月网络期刊，黑客期刊发布
请将本站推荐给更多的好友
让大家都成为溜客一员**

溜客資料共享群：

**访问溜客安全网最下方
查看本站最新共享QQ群**

**做一个通过正道可以养活自己的黑客
从我做起，不做伪黑客**

目录

01 黑客基础知识

1.1 揭开黑客的神秘面纱	2
1.1.1 黑客的兴起	2
1.1.2 黑客的组成	2
1.1.3 黑客的主要行为	3
1.2 认识 IP 地址	4
1.2.1 IP 地址的表示方法	4
1.2.2 IP 地址的分类	4
1.3 认识端口	5
1.3.1 端口的分类	5
1.3.2 查看系统的开放端口	7
1.3.3 关闭不必要的端口	8
1.3.4 限制访问指定的端口	9
1.4 了解黑客常用的命令	13
1.4.1 ping 命令	13
1.4.2 net 命令	15
1.4.3 netstat 命令	19
1.4.4 ftp 命令	20
1.4.5 telnet 命令	22
1.4.6 ipconfig 命令	22
1.5 创建安全的测试环境	23
1.5.1 安装 VMware 虚拟机	23
1.5.2 创建虚拟机	25
1.5.3 在虚拟机中安装操作系统	28

02 常用扫描与嗅探工具

2.1 了解扫描目标的相关信息	33
2.1.1 确定目标的 IP 地址	33
2.1.2 查看目标所属地区	33
2.2 认识扫描器	34
2.2.1 扫描器的工作原理	34
2.2.2 扫描器的作用	34
2.3 常见端口扫描器	35
2.3.1 Nmap 扫描器	35

2.3.2 SuperScan 扫描器	38
2.4 常见多功能扫描器	41
2.4.1 流光扫描器	41
2.4.2 SSS 扫描器	46
2.4.3 X-Scan 扫描器	52
2.5 常用网络嗅探工具	54
2.5.1 嗅探利器 SmartSniff	54
2.5.2 Iris 网络嗅探器	55
2.5.3 网络数据包嗅探专家	58
2.5.4 影音神探	60

03 Windows 系统漏洞攻防

3.1 认识系统漏洞	62
3.1.1 什么是系统漏洞	62
3.1.2 系统漏洞产生的原因	62
3.2 Windows 中存在的系统漏洞 ...	62
3.3 系统漏洞的监测与修复	68
3.3.1 利用 Windows 自动更新 软件	68
3.3.2 使用 360 安全卫士	70
3.3.3 使用瑞星卡卡上网 安全助手	72
3.3.4 使用金山系统漏洞 修补工具	72

04 设置系统安全策略

4.1 设置本地安全策略	75
4.1.1 禁止在登录前关机	75
4.1.2 在超过登录时间后强制用户 注销	76
4.1.3 不显示上次登录时的 用户名	76
4.1.4 限制格式化和弹出 可移动媒体	77

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



4.1.5	对备份和还原权限进行审计.....	78
4.1.6	禁止在下次更改密码时存储 LAN Manager 的 Hash 值....	78
4.1.7	设置本地账户共享与安全模式.....	79
4.1.8	禁止安装未签名的驱动程序.....	80
4.1.9	不允许 SAM 账户和共享的匿名枚举.....	80
4.1.10	让“每个人”权限应用于匿名用户.....	81
4.1.11	定义 IP 安全策略.....	82
4.2	设置组策略.....	85
4.2.1	设置账户锁定策略.....	85
4.2.2	设置密码策略.....	86
4.2.3	设置用户权限.....	88
4.2.4	更改系统默认的管理员账户.....	89
4.2.5	不允许 SAM 账户的匿名枚举.....	90
4.2.6	禁止访问控制面板.....	90
4.2.7	禁止更改“开始”菜单.....	91
4.2.8	禁止更改桌面设置.....	91
4.2.9	禁止访问指定的磁盘驱动器.....	92
4.2.10	禁用部分应用程序.....	92
4.3	设置计算机管理策略.....	94
4.3.1	事件查看器的使用.....	94
4.3.2	共享资源的管理.....	95
4.3.3	管理系统中的服务程序.....	96
4.4	设置注册表编辑器安全.....	97
4.4.1	禁止访问和编辑注册表.....	97
4.4.2	禁止远程修改注册表.....	101
4.4.3	禁止运行应用程序.....	101
4.4.4	禁止更改系统登录密码.....	102
4.4.5	隐藏控制面板中的图标.....	103
4.4.6	禁止 IE 浏览器查看本地磁盘.....	104

4.4.7	关闭默认共享.....	105
-------	-------------	-----

05 系统与文件加密

5.1	为操作系统加密.....	107
5.1.1	设置 CMOS 开机密码.....	107
5.1.2	设置系统启动密码.....	108
5.1.3	设置屏幕保护密码.....	109
5.2	为文件加密.....	111
5.2.1	为 Word 文档加密.....	111
5.2.2	为 Excel 表格加密.....	111
5.2.3	为 WPS Office 文档加密... ..	112
5.2.4	为电子邮件加密.....	113
5.2.5	为压缩文件加密.....	114
5.3	使用加密软件加密.....	115
5.3.1	文本文件专用加密器.....	115
5.3.2	文件夹加密精灵.....	117
5.3.3	终极程序加密器.....	119
5.3.4	万能加密器.....	120
5.4	破解管理员账户.....	125
5.4.1	使用 Administrator 账户登录.....	125
5.4.2	强制清除管理员密码.....	126
5.4.3	创建密码恢复盘.....	126
5.4.4	使用密码恢复软件.....	128

06 远程控制攻防

6.1	基于认证入侵.....	131
6.1.1	IPC\$入侵与防范.....	131
6.1.2	Telnet 入侵概述.....	137
6.2	通过注册表入侵.....	140
6.2.1	开启远程注册表服务.....	140
6.2.2	修改注册表实现远程监控... ..	142
6.3	Windows XP 远程控制.....	143
6.3.1	Windows XP 系统的远程协助.....	143
6.3.2	Windows XP 远程关机.....	144
6.4	使用网络执法官.....	146

目录 [Contents]

6.4.1 网络法官的功能	146
6.4.2 认识网络法官的操作 界面	147
6.4.3 网络法官的常用操作	148
6.5 使用远程控制软件	150
6.5.1 网络人（Netman）的 功能	150
6.5.2 网络人（Netman）的 使用	151

07 木马攻防

7.1 木马基础知识	155
7.1.1 木马的概念和结构	155
7.1.2 木马的分类	156
7.1.3 木马的特点	157
7.1.4 木马的入侵和启动	158
7.1.5 木马的伪装手段	160
7.2 木马的制作	161
7.2.1 使用“EXE 捆绑机”捆绑 木马	162
7.2.2 自解压木马	163
7.2.3 网页木马生成器	165
7.2.4 CHM 电子书木马	166
7.3 木马的清除与防范	168
7.3.1 木马清道夫清除木马	168
7.3.2 木马克星 Ipmor 清除木马	170
7.3.3 金山贝壳木马专杀 清除木马	171
7.3.4 手动查杀系统中的 隐藏木马	172
7.3.5 常见木马防范措施	173
7.4 “冰河”木马的使用	175
7.4.1 配置“冰河”木马的服务器 端程序	175
7.4.2 使用“冰河”木马控制远程 计算机	176
7.4.3 卸载和清除“冰河”木马	178

7.5 认识“广外女生”木马与清除 该木马	180
7.5.1 “广外女生”木马的使用	180
7.5.2 “广外女生”木马的清除	182

08 聊天软件攻防

8.1 常见 QQ 攻击方式	184
8.1.1 强制聊天	184
8.1.2 利用“炸弹”攻击	184
8.1.3 破解本地 QQ 密码	185
8.1.4 本地记录查询	186
8.1.5 非法获取用户 IP	187
8.1.6 QQ 尾巴病毒	188
8.2 保护好自己的 QQ	189
8.2.1 设置 QQ 密码保护	190
8.2.2 防范 IP 地址被探测	193
8.2.3 利用“QQ 医生”保护 QQ 安全	194
8.2.4 加密聊天记录	196
8.3 MSN 的攻击与防御	197
8.3.1 针对 MSN 的攻击	197
8.3.2 MSN 聊天加密	199
8.3.3 Windows Live Messenger 保护盾	200

09 网页恶意代码攻防

9.1 恶意代码简介	203
9.1.1 恶意代码概述	203
9.1.2 WSH 知识	203
9.1.3 恶意代码的特征	204
9.1.4 非过滤性病毒	204
9.1.5 恶意代码的传播方式	204
9.2 恶意代码的预防和清除	205
9.2.1 恶意代码的预防	205
9.2.2 恶意代码的清除	205
9.3 常见恶意代码及解决方法	207
9.3.1 启动时自动弹出对话框和 网页	207



9.3.2	修改起始页和默认主页	208
9.3.3	强行修改 IE 标题栏	208
9.3.4	强行修改右键菜单	209
9.3.5	禁用注册表	210
9.4	IE 浏览器安全维护	210
9.4.1	IE 浏览器安全设置	211
9.4.2	更新系统漏洞补丁	214
9.4.3	用“360 安全卫士”修复 IE 浏览器	216
9.4.4	使用“瑞星卡卡上网助手”	217

10 电子邮件攻防

10.1	电子邮件病毒	224
10.1.1	“邮件病毒”定义及特征	224
10.1.2	识别“邮件病毒”	224
10.2	认识电子邮件炸弹	225
10.2.1	电子邮件炸弹的定义和危害	225
10.2.2	电子邮件炸弹的制作	226
10.3	常见获取电子邮件密码手段	226
10.3.1	使用流光	227
10.3.2	使用“溯雪 Web 密码探测器”	228
10.3.3	使用“黑雨”软件暴力破解	229
10.3.4	使用“流影”破解邮箱密码	230
10.4	防范电子邮件攻击	231
10.4.1	重要邮箱的保护措施	231
10.4.2	找回邮箱密码	232
10.4.3	防止炸弹攻击	233
10.5	防范电子邮件病毒	234
10.5.1	设置邮件的显示格式	234
10.5.2	设置 Outlook Express	235
10.5.3	变更文件关联	237

11 U 盘病毒攻防

11.1	U 盘病毒概述	240
11.1.1	U 盘病毒的原理和特点	240
11.1.2	常见 U 盘病毒	240
11.2	U 盘病毒的防御	241
11.2.1	使用组策略关闭“自动播放”功能	241
11.2.2	修改注册表关闭“自动播放”功能	242
11.2.3	设置服务关闭“自动播放”功能	243
11.2.4	使用安全的操作方法	244
11.3	autorun.inf 解析	244
11.4	U 盘病毒的查杀	245
11.4.1	用 WinRAR 查杀 U 盘病毒	245
11.4.2	U 盘病毒的手动删除	246
11.4.3	U 盘病毒专杀工具——USBCleaner	247
11.4.4	U 盘病毒专杀工具——USBKiller	249

12 使用电脑安全软件

12.1	使用杀毒软件清除电脑病毒	254
12.1.1	金山毒霸的使用	254
12.1.2	卡巴斯基的使用	256
12.1.3	瑞星杀毒软件的使用	259
12.1.4	NOD32 的使用	264
12.1.5	Norton AntiVirus 的使用	265
12.2	清理电脑中的恶意软件	267
12.2.1	恶意软件的特征	267
12.2.2	常用恶意软件清理工具	268
12.3	使用防火墙抵御网络攻击	269
12.3.1	Windows 系统自带的防火墙	269

目录 Contents

12.3.2 “天网”个人防火墙.....272

12.3.3 ZoneAlarm 个人网络
防火墙.....279

13 黑客攻防实用技巧

13.1 系统设置与账户管理技巧283

13.1.1 Windows XP 中常见的
系统进程283

13.1.2 关闭系统的所有端口283

13.1.3 禁止随机启动程序284

13.1.4 禁用远程协助功能285

13.1.5 设置注册表管理权限285

13.1.6 禁用组策略功能287

13.1.7 启用组策略功能288

13.1.8 禁用“Windows 任务
管理器”288

13.1.9 禁用的命令提示符289

13.1.10 找出系统隐藏的
超级用户290

13.1.11 改变计算机管理员账户
Administrator 名称290

13.1.12 为自己分配管理员权限....291

13.1.13 让系统文件彻底不显示....291

13.1.14 删除无关用户账户292

13.1.15 禁止访问“控制面板”293

13.1.16 将“我的文档”转移到
非系统分区.....293

13.2 系统应用与故障排除技巧294

13.2.1 关机时清空页面文件294

13.2.2 创建锁定计算机的快捷
方式294

13.2.3 关闭 Windows XP 的
自动播放功能295

13.2.4 自行配置 Windows XP 的
服务296

13.2.5 恢复误删除的 boot.ini 文件296

13.2.6 自动关闭停止响应的程序297

13.2.7 删除 Windows XP 的
“更新”选项297

13.2.8 恢复被破坏的系统引导
文件.....298

13.2.9 无法打开注册表.....298

13.2.10 将自动更新页面改为
中文.....299

13.2.11 无法设置共享文件的访问
权限.....300

13.2.12 恢复 Windows XP 系统的
输入法浮动条300

13.3 IE 浏览器安全应用技巧301

13.3.1 清除地址栏中浏览过的
网址和中文实名地址.....301

13.3.2 恢复鼠标右键的复制和
粘贴功能.....302

13.3.3 恢复 IE 浏览器默认首页 ...302

13.3.4 管理 Internet 加载项.....303

13.3.5 设置 IE 浏览器拒绝运行
Java 小程序脚本.....303

13.3.6 隐藏 IE 地址栏.....304

13.3.7 解除 IE 的分级审查口令 ...305

13.3.8 禁止 IE 访问某些站点.....305

13.4 常见病毒和木马的防范
技巧306

13.4.1 指定 Windows 防火墙阻止
所有未经请求的传入消息...306

13.4.2 处理感染病毒的计算机....306

13.4.3 定期检查敏感文件306

13.4.4 识别隐藏的木马程序
原文件307

13.4.5 木马程序对通信端口的
使用.....307

13.4.6 木马程序隐藏运行进程的
方法.....308

13.4.7 通过修改文件关联启动
木马程序.....309

13.4.8 防范木马的常用方法309

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

**你
想
换
吗
？**

www.17huan.com

Chapter

01

黑客基础知识

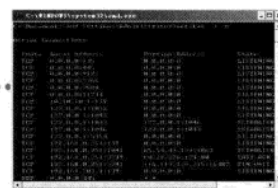
随着网络技术的不断发展，人们的日常生活和工作越来越离不开网络，互联网给我们带来了极大便利，但随之出现的网络安全问题也成为用户最为头痛的事情。在学习黑客攻防技术之前，首先我们来了解一些关于黑客的基础知识，认识 IP 地址、端口和一些黑客常用的 DOS 命令，最后创建一个安全的测试环境。

本章建议学习时间：

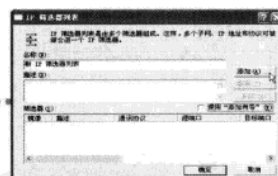
本章建议学习时间为 50 分钟，其中分配 15 分钟学习黑客、IP 地址和端口基础知识，15 分钟了解黑客常用的命令，20 分钟用于学习创建安全的测试环境。

学完本章后您可以：

- 了解黑客的行为
- 认识 IP 地址
- 认识端口
- 了解黑客的常用命令
- 创建安全的测试环境



查看端口状态



IP 筛选器列表



输入 ping 命令



重要知识点视频索引



1.1 揭开黑客的神秘面纱

谈到网络安全，人们不自觉地就会联想到黑客，人们往往会将他们同破坏网络安全、盗取用户账号、偷窃个人私密信息等行为联系起来。其实黑客也有好坏之分，他们并不全是网络上的捣乱分子，其中也有一部分是网络上的安全卫士。下面我们就来揭开黑客的神秘面纱，让用户详细了解黑客到底是一群什么样的人。

在黑客圈中，Hacker 一词早期是带有正面意义的，但到了今天，“黑客”一词已经成为那些专门利用电脑进行破坏或入侵他人电脑的人的代名词，其实对这种人正确的叫法应该是 Cracker，有人翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体。黑客和骇客根本的区别是：黑客们修补系统漏洞，而骇客们利用系统漏洞进行破坏。

1.1.1 黑客的兴起

黑客最早出现于 20 世纪 50 年代，最早的计算机于 1946 年在宾夕法尼亚大学出现，而最早的黑客则出现于麻省理工学院，贝尔实验室也有。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由，并主张信息的共享。

1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着电脑的普及和因特网技术的迅速发展，现代意义上的黑客也随之出现。

“黑客”一词一般有以下四种意义：

- ❖ 一个对（某领域内的）编程语言有足够了解，可以不经长时间思考就能创造出有用的软件的人。
- ❖ 一个试图恶意（一般是非法地）破解或破坏某个程序、系统及网络安全的人。这个意义常常对那些符合上个条件的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”。
- ❖ 一个试图破解某系统或网络，以提醒该系统所有者及其电脑系统的安全漏洞，这群人往往被称做“红客”。许多这样的人是电脑安全公司的雇员，并在完全合法的情况下攻击某系统。
- ❖ 一个通过知识或猜测而对某段程序做出（往往是好的）修改，并改变（或增强）该程序用途的人。

现在，网络上出现了越来越多的 Cracker，他们只是入侵，使用扫描器到处乱扫，用 IP 炸弹轰炸，毫无目的地入侵、破坏，他们并无益于电脑技术的发展，反而有害于网络的安全，造成网络瘫痪，给人们带来巨大的经济和精神损失。

1.1.2 黑客的组成

到了今天，黑客已经不像以前那样是少数现象，他们已经发展成网络上的一个独特的群

Chapter 01 黑客基础知识

体。他们有着与常人不同的思维方法，有着自己独特的行为方式，网络上现在出现了很多由一些志同道合的人组织起来的黑客组织。但是这些人是从什么地方来的呢？他们是什么样的人？其实除了极少数的职业黑客以外，大多数黑客都是业余的，而黑客其实和现实中的平常人没有区别，或许他就是一个普通的高中在读学生。

有人曾经对黑客年龄这方面进行过调查，组成黑客的主要群体是 18~30 岁之间的年轻人，大多是男性，不过现在有很多女性也加入到这个行列。他们大多是在校的学生，因为他们有着很强的电脑爱好和很多自由时间，好奇心强、精力旺盛等使他们步入了黑客的行列。还有一些黑客有自己的事业或工作，包括程序员、资深安全员、安全研究员、职业间谍、安全顾问等。当然这些人的技术水平与刚刚入门的“小黑客”无法相比，不过他们也是从新手一步步地走过来的。

1.1.3 黑客的主要行为

“黑客”大体上应该分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善；邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情。

无论哪类黑客，他们最初的学习内容都是本书所涉及的内容，而且掌握的基本技能也都是是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

黑客的行为主要有以下几种：

其一，学习技术。互联网上的新技术一旦出现，黑客就立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术的机理。一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客”身份超过一年。

其二，伪装自己。黑客的一举一动都会被服务器记录下来，所以黑客都会伪装自己，使得对方无法辨别其真实身份。这需要熟练的技巧，还有用来伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，初学者不可能在短时间内学会。

其三，发现漏洞。漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然，他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

其四，利用漏洞。对于正派黑客来说，漏洞要被修补；对于邪派黑客来说，漏洞要用来搞破坏。

作为一名黑客，道德是非常重要的，这往往决定一个黑客的前途和命运。如果开始学习的时候就是为了扬名或非法获利，那就不能称之为黑客。但是，虚拟的网络世界不能用现实中的规范去管理，而黑客又是在这个虚拟世界里最渴望自由和共享的。虽然网络上的黑客道德或守则出现很多，也有很多黑客章程，但是这些所谓的道德往往成为一纸空文，黑客们真正遵守的是来自内心真诚的道德，是一种信仰，而不是人为的、外在的一种守则。也只有这些来自于黑客们内心的道德才可以真正地约束他们。

现在有不少人以盗取他人的游戏账号、银行卡号，窃取公司机密，攻击别人网站，敲诈，

基础知识

常用扫描
与嗅探工具

Windows系
统漏洞攻防

设置系统
安全策略

系统与文
件加密

远程控
制攻防

木马
件攻防

聊天软
件攻防

网页恶
意代码防

电子邮
件攻防

C语言
病毒攻防

使用电脑
安全软件

黑客攻
防技巧



欺骗等非法获利，这些人都不能称之为“黑客”，对于他们应该称为“骇客”更为合适，他们最终会受到法律的制裁和良心的谴责。

1.2 认识 IP 地址

用户都知道，在我们常用的电话通信中，电话用户是靠电话号码来识别的。同样，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP 地址”。下面一起来认识一下 IP 地址。

1.2.1 IP 地址的表示方法

IP 地址就像是我们的家庭住址一样，如果你要写信给一个人，你就要知道他（她）的地址，这样邮递员才能把信送到。计算机发送信息时就好像邮递员，它必须知道唯一的“家庭地址”才不至于把信送错人家。所不同的是，我们的地址使用文字来表示，而计算机的地址用二进制数字表示。

IP 地址的长度为 32 位，分为 4 个字节，每个字节对应 8 位二进制位，即每部分数字不超过 $2^8=256$ 。例如，一个用二进制形式记录的 IP 地址可以表示为：11000000 10011110 00000011 00000101。

为了方便使用，IP 地址的每个字节通常用十进制形式表示，每段数字范围为 0~255，段与段之间用句点隔开，如上面的 IP 地址就可以表示为：192.158.3.5。IP 地址的这种表示方法叫做“点分十进制表示法”，这显然比大量 1 和 0 容易记忆得多。

1.2.2 IP 地址的分类

最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址分为网络地址和主机地址两部分。同一个物理网络上的所有主机都使用同一个网络地址，而同一网络上的一个主机都有一个主机地址与其对应。

IP 地址根据网络 ID 的不同分为 5 种类型，即 A 类地址、B 类地址、C 类地址、D 类地址和 E 类地址。

1. A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，地址范围为：1.0.0.1~126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001~01111110 11111111 11111111 11111110）。可用的 A 类网络有 126 个，每个网络能容纳 1 677 214 台主机。

2. B 类 IP 地址

一个 B 类 IP 地址由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是“10”，地址范围为：128.1.0.1~191.255.255.254（二进制表示为：10000000 00000001 00000000 00000001~10111111 11111111 11111111 11111110）。可用的 B 类网络有 16 384 个，每个网络能容纳 65 534 台主机。

Chapter 01 黑客基础知识

3. C 类 IP 地址

一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是 110，地址范围为 192.0.1.1~223.255.255.254（二进制表示为：11000000 00000000 00000001 00000001~11011111 11111111 11111111 11111110）。C 类网络可达 2 097 152 个，每个网络能容纳 254 个主机。

4. D 类 IP 地址

D 类 IP 地址第一个字节以 1110 开始，地址范围为：224.0.0.1~239.255.255.254。它是一个专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

5. E 类 IP 地址

E 类地址仅作实验和将来开发而保留，它以 1111 开始，全 0（0.0.0.0）的 IP 地址指任意网络，全 1 的 IP 地址（255.255.255.255）是当前子网的广播地址，如下图所示。

	0	1	2	3	4	5	6	7	8	15	16	23	24	31
A 类	0													
B 类	10													
C 类	110													
D 类	1110													
E 类	11110													

1.3 认识端口

计算机“端口”（port）可以认为是计算机与外界通信交流的出口，其中硬件领域的端口又称接口，如 USB 端口、串行端口等；软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入/输出）缓冲区。

在网络技术中，端口（port）有多种含义。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。这里所指的端口不是物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

如果把 IP 地址比作一间房子，TCP/IP 协议中的端口指的就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65 536（即 256×256）个。端口是通过端口号来标记的，端口号只有整数，范围是 0~65 535（256×256-1）。

1.3.1 端口的分类

计算机中的端口按不同的标准可以分为很多类，其中最常用的分类标准有以下两种：

1. 按端口号分布划分

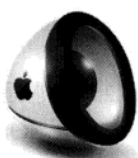
按端口号分布划分，可以将端口分为三大类，分别为：公认端口、注册端口和动态/私有端口。

黑客基础知识
常用扫描工具
与嗅探工具
系统漏洞攻防
Windows 系统
设置系统
安全策略
系统加密
远程控制
木马
聊天软件
网页恶意
代码攻防
电子邮件
病毒攻防
使用电脑
黑客攻防
实用技巧



（1）公认端口

公认端口是指那些用户所熟知的端口号，范围为 0~1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80 端口分配给 WWW 服务，21 端口分配给 FTP 服务等。



提示

我们在 IE 浏览器的地址栏中输入一个网址的时候是不必指定端口号的，因为在默认情况下 WWW 服务的端口号是 80。

（2）注册端口

注册端口（registered ports）的端口号为 1024~49151。它们松散地绑定于一些服务，也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的。这些端口大多数没有明确的定义服务对象，应用程序可以根据自己的需要进行定义。例如，我们常用的聊天软件腾讯 QQ 用的就是 4000 端口。

（3）动态/私有端口

动态/私有端口（dynamic/private ports）的端口号为 49152~65535。理论上，不应为服务分配这些端口。但实际上一些较为特殊的程序，特别是一些木马程序常常使用这些端口，因为它们通常从 1024 起分配动态端口而不被人们注意，容易隐藏，如 SUN 的 RPC 端口就是从 32768 端口开始的。

2. 按通信服务方式划分

计算机通信的连接方式有以下两种：

第一种是直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用 TCP 协议。

第二种是不直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达，也就是“无连接方式”。这种方式大多采用 UDP 协议，IP 协议也是一种无连接方式。

对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP 协议端口”和“UDP 协议端口”。计算机之间相互通信一般采用这两种通信协议。

使用 TCP 协议的常见端口主要有以下几种：

❖ FTP：定义了文件传输协议，使用 21 端口。用户常说某计算机开启了 FTP 服务，便是启动了文件传输服务，下载文件、上传主页都要用到 FTP 服务。

❖ Telnet：它是一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。早期的 BBS 是纯字符界面，支持 BBS 的服务器将 23 端口打开，对外提供服务。

❖ SMTP：定义了简单邮件传送协议，现在很多邮件服务器用的都是这个协议，用于发送邮件。常见的免费邮件服务用的就是这个邮件服务端口，所以在电子邮件设置中常看到有 SMTP 端口设置栏，服务器开放的是 25 端口。

❖ POP3：它和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也就是说，只要有相应的使用 POP3 协议的程序（如 Foxmail 或 Outlook），就可以不以

Chapter 01 黑客基础知识

Web 方式登录邮箱界面，直接用邮件程序就可以收到邮件（如果是 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。

使用 UDP 协议的端口常见的有：

- ❖ HTTP：这是用户用得最多的协议，它就是常说的“超文本传输协议”。上网浏览网页时，就得在提供网页资源的计算机上打开 80 端口以提供服务，常见的“WWW 服务”、“Web 服务器”用的就是这个端口。

- ❖ DNS：用于域名解析服务，这种服务在 Windows NT 系统中用得最多。因特网上的每一台计算机都有一个网络地址与之对应，这个地址就是常说的 IP 地址，它以纯数字+“.”的形式表示。然而这不便记忆，于是出现了域名，访问计算机的时候只需要知道域名，域名和 IP 地址之间的变换由 DNS 服务器来完成。DNS 用的是 53 端口。

- ❖ SNMP：简单网络管理协议，使用 161 端口，用来管理网络设备。由于网络设备很多，无连接的服务就体现出其优势。

- ❖ QQ：QQ 程序既接受服务，又提供服务，这样两个聊天的人才平等的。QQ 用的是无连接的协议，也就是说它用的是 UDP 协议。QQ 服务器使用 8000 端口，侦听是否有信息到来，客户端使用 4000 端口，向外发送信息。如果上述两个端口正在使用（有很多人同时和几个好友聊天），就顺序往上加。

另外，代理服务器常用以下端口：

- ❖ HTTP 协议代理服务器常用端口：80/8080/3128/8081/9080。
- ❖ SOCKS 代理协议服务器常用端口：1080。
- ❖ FTP 协议代理服务器常用端口：21。
- ❖ Telnet 协议代理服务器常用端口：23。

1.3.2 查看系统的开放端口

通过了解系统开放端口的状态变化，可以帮助我们更好地保护系统、防范黑客入侵、保证电脑安全。用户可以使用 netstat 命令查看自己系统端口的状态，了解系统当前开放了哪些端口。使用 netstat 命令查看系统端口的具体操作步骤如下：

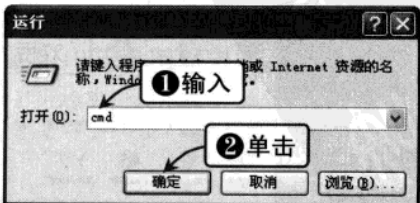
STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，打开“运行”对话框，如下图所示。



STEP 02 输入 cmd 命令

在“打开”下拉列表框中输入 cmd 命令，然后单击“确定”按钮，打开“命令提示符”窗口，如下图所示。





STEP 03 输入 netstat -a -n 命令

在打开的“命令提示符”窗口中，输入 netstat -a -n 命令，如下图所示。



STEP 04 查看端口状态

按【Enter】键，即可看到以数字显示的 TCP 和 UDP 连接的端口号及其状态，如下图所示。



提示

关于 netstat 命令的使用方法及其参数的具体含义我们将在后面的内容中进行详细介绍，在此不再赘述。

1.3.3 关闭不必要的端口

在系统默认情况下，用户系统中有很多没用或不安全的端口是开启的，这些端口很容易被黑客利用，为了保障系统安全，可以将这些不用的端口关闭。

下面以关闭 Remote Desktop Help Session Manager（Windows 远程协助服务）为例进行介绍，其具体操作步骤如下：

STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令打开“控制面板”窗口，双击“管理工具”图标，如下图所示。



STEP 02 打开“管理工具”窗口

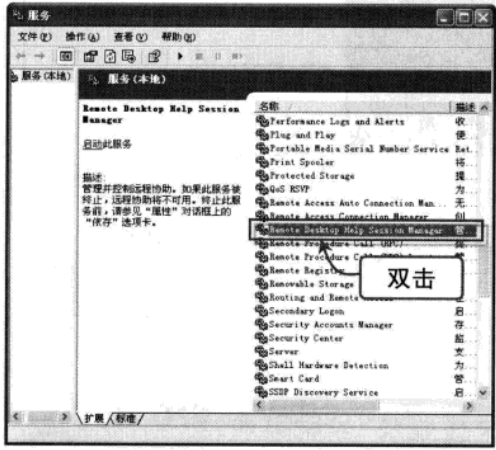
打开“管理工具”窗口，双击“服务”图标，如下图所示。



Chapter 01 黑客基础知识

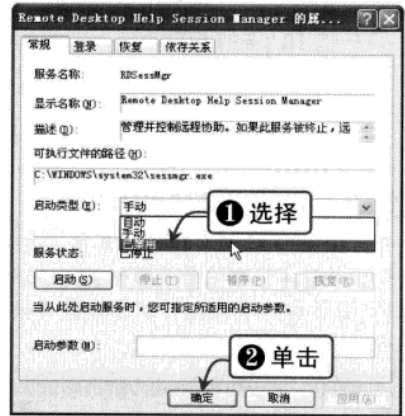
STEP 03 打开“服务”窗口

打开“服务”窗口，找到 Remote Desktop Help Session Manager 服务项，双击该服务项，如下图所示。



STEP 04 禁用该服务项

弹出“Remote Desktop Help Session Manager 的属性”对话框，在“启动类型”下拉列表框中选择“已禁用”选项，然后单击“确定”按钮禁用该服务项，如下图所示。



1.3.4 限制访问指定的端口

通过限制访问指定的端口，同样可以达到关闭端口的目的。下面以限制访问 3389 端口（黑客常常利用该端口远程控制用户的主机，使其成为“3389 肉鸡”）为例进行介绍，具体操作步骤如下：

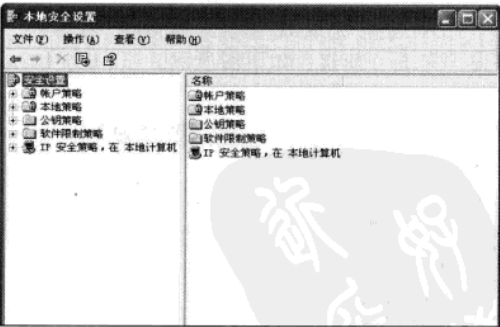
STEP 01 打开“管理工具”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，打开“管理工具”窗口，如下图所示。



STEP 02 打开“本地安全设置”窗口

在“管理工具”窗口中双击“本地安全策略”图标，打开“本地安全设置”窗口，如下图所示。



STEP 03 创建 IP 安全策略

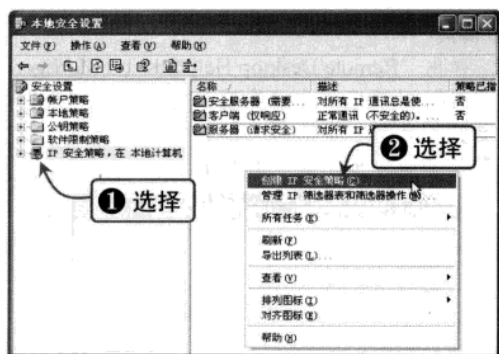
在左侧窗格中选择“IP 安全策略”，在本地计算机”选项，在右侧窗格中右击，在弹出的快捷菜单中选择“创建 IP 安全策略”选项，如下图所示。

STEP 04 IP 安全策略向导

打开“欢迎使用‘IP 安全策略向导’”对话框，单击“下一步”按钮，如下图所示。

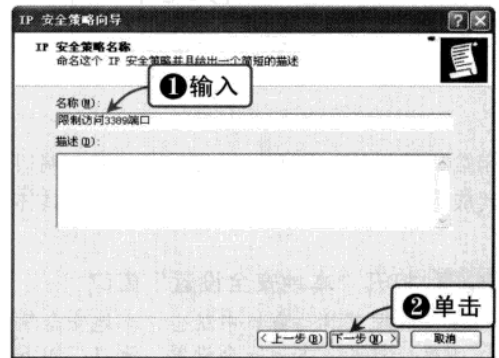
- 黑客基础知识
- 常用扫描工具
- 系统漏洞扫描
- 设置系统安全策略
- 系统与文件加密
- 远程控制
- 木马攻击
- 聊天软件攻击
- 网页恶意代码攻击
- 电子邮件攻击
- C 盘病毒攻击
- 使用电脑安全软件
- 黑客攻防实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



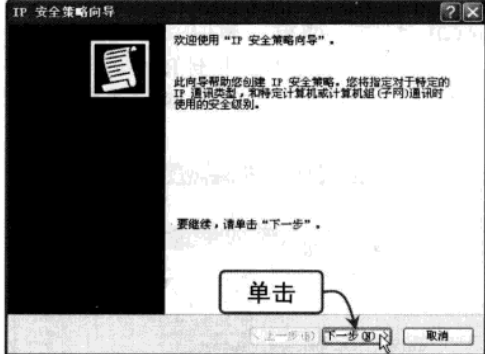
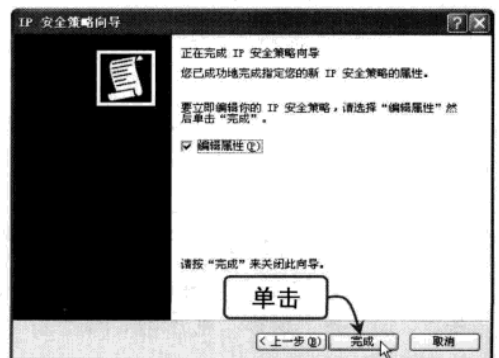
STEP 05 输入 IP 安全策略名称

打开“IP 安全策略名称”对话框，在“名称”文本框中输入策略名称“限制访问 3389 端口”，如下图所示。用户也可以保持默认设置，然后单击“下一步”按钮。



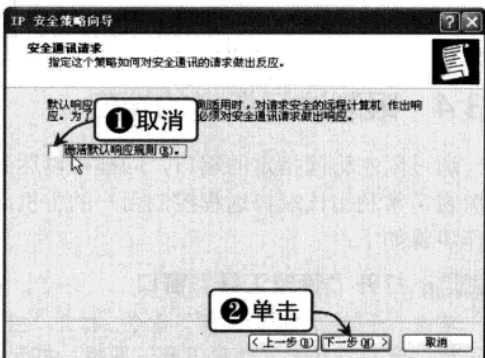
STEP 07 完成 IP 安全策略向导

打开“正在完成 IP 安全策略向导”对话框，单击“完成”按钮，如下图所示。



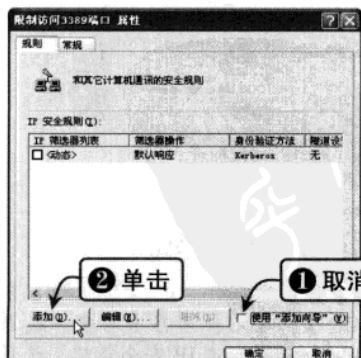
STEP 06 “安全通讯请求”对话框

打开“安全通讯请求”对话框，取消选择“激活默认响应规则”复选框，然后单击“下一步”按钮，如下图所示。



STEP 08 设置限制访问端口属性

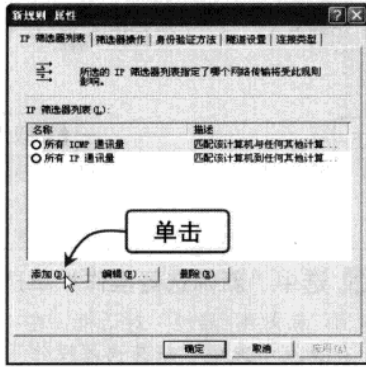
打开“限制访问 3389 端口 属性”对话框，取消选择“使用‘添加向导’”复选框，并单击“添加”按钮，如下图所示。



Chapter 01 黑客基础知识

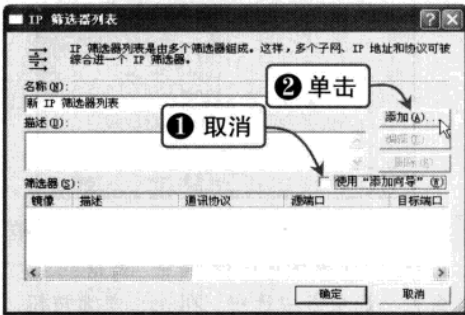
STEP 09 “新规则 属性”对话框

打开“新规则 属性”对话框，单击“添加”按钮，如下图所示。



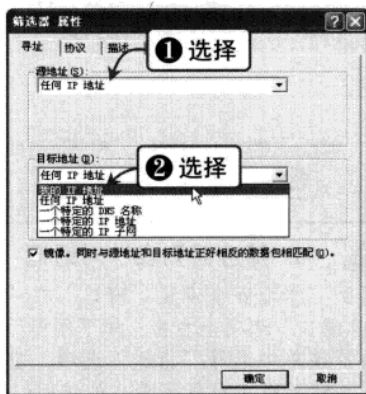
STEP 10 “IP 筛选器列表”对话框

打开“IP 筛选器列表”对话框，取消选择“使用‘添加向导’”复选框，单击“添加”按钮，如下图所示。



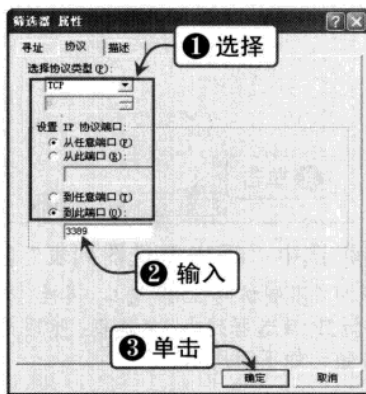
STEP 11 “筛选器 属性”对话框

打开“筛选器 属性”对话框，在“源地址”下拉列表框中选择“任何 IP 地址”选项，在“目标地址”下拉列表框中选择“我的 IP 地址”选项，如下图所示。



STEP 12 选择协议类型

选择“协议”选项卡，在“选择协议类型”下拉列表框中选择 TCP 选项，选中“从任意端口”和“到此端口”单选按钮，并在下面的文本框中输入 3389，单击“确定”按钮，如下图所示。



提示



在“筛选器 属性”对话框中，“源地址”为发来数据包的地址，“目标地址”为接收数据包的地址，用户可以在这两个下拉列表框中选择“我的 IP 地址”、“任何 IP 地址”、“一个特定的 DNS 名称”等选项。

STEP 13 返回“新规则 属性”对话框

返回“IP 筛选器列表”对话框，单击“添加”按钮可继续添加限制端口，单击“确定”按钮返回“新规则 属性”对话框，选中“新 IP 筛选器列表”单选按钮，如下图所示。

STEP 14 “筛选器操作”选项卡

选择“筛选器操作”选项卡，取消选择“使用‘添加向导’”复选框，单击“添加”按钮，如下图所示。

基础知识

与嗅探工具

统编洞攻防

安全策略

件加密

制攻防

件攻防

代码攻防

件攻防

毒攻防

安全软件

实用技巧



STEP 15 “新筛选器操作 属性”对话框

弹出“新筛选器操作 属性”对话框，在“安全措施”选项卡中选中“阻止”单选按钮，然后单击“确定”按钮，如下图所示。

STEP 17 选中“新 IP 筛选器列表”复选框

返回“限制访问 3389 端口”属性对话框，选中“新 IP 筛选器列表”复选框，然后单击“关闭”按钮，如下图所示。

STEP 16 选中“新筛选器操作”单选按钮

返回“新规则 属性”对话框，在“筛选器操作”列表框中选中“新筛选器操作”单选按钮，然后单击“关闭”按钮，如下图所示。

STEP 18 “IP 筛选器列表”对话框

返回“本地安全设置”窗口，在“限制访问 3389 端口”选项上右击，如下图所示。在弹出的快捷菜单中选择“指派”选项，重新启动计算机，即可阻止对指定端口的访问。

1.4 了解黑客常用的命令

要想成为一名黑客，首先要记住一些常用的 DOS 命令，并熟练掌握这些命令的使用方法，下面就来简单介绍一些黑客常用的命令及其使用方法。

1.4.1 ping 命令

ping 是用来检查网络是否畅通或者网络连接速度的命令。作为一个生活在网络上的管理员或者黑客来说，ping 命令是第一个必须掌握的 DOS 命令。

ping 命令所利用的原理是：网络上的计算机都有一个唯一确定的 IP 地址，我们给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包我们可以确定目标主机的存在，可以初步判断目标主机的操作系统等。

按照系统默认设置，Windows 上运行的 ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个数据 32 字节，如果一切正常，应该能得到 4 个回送应答。ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器即网络连接速度比较快。

ping 还能显示 TTL（Time To Live，存在时间）值，用户可以通过 TTL 值推算一下数据包已经通过了多少个路由器，公式如下：

源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）- 返回时 TTL 值

例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段（128~119）；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 10 个路由器网段。

在一般情况下还可以通过返回给你的 TTL 值大小，粗略判断目标主机的系统类型是 Windows 系列还是 UNIX/Linux 系列，一般情况下 Windows 系列的系统返回的 TTL 值在 100~130 之间，而 UNIX/Linux 系列的系统返回的 TTL 值在 240~255 之间。

ping 命令的主要作用是通过发送数据包并接收应答信息来检测两台计算机之间的网络是否连通。当网络出现故障的时候，可以用这个命令来预测故障和确定故障地点。ping 命令成功只是说明当前主机与目的主机之间存在一条连通的路径。如果不成功，则需要考虑网线是否连通、网卡设置是否正确、IP 地址是否可用等情况。



提示

ping 命令指的是端对端连通，通常用于网络可用性检查，但是某些病毒木马会强行大量远程执行 ping 命令抢占你的网络资源，导致系统变慢，网速变慢。

在 Windows XP 操作系统环境下，利用 ping 命令测试网络连通状态的具体方法如下：

STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，打开“运行”对话框，如下图所示。

STEP 02 打开“命令提示符”窗口

在“打开”下拉列表框中输入 cmd 命令，单击“确定”按钮，打开“命令提示符”窗口，如下图所示。

基础
知识

常用
扫描
与嗅探
工具

漏洞
扫描
系统

安全
策略

系统
与文
件加
密

远程
控制

木马
攻击

聊天
软件
攻击

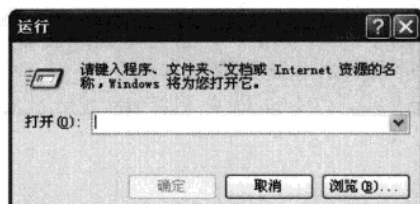
网页
攻击

电子
邮件
攻击

病毒
攻击

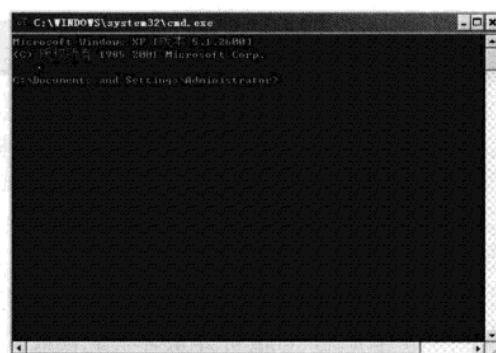
使用
电脑
安全
软件

黑客
攻击
实用
技巧



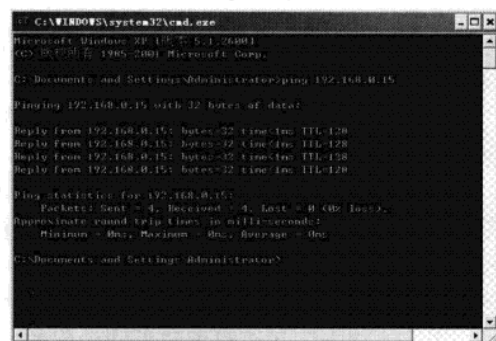
STEP 03 输入 ping 命令

在“命令提示符”窗口中输入 ping 命令，其格式为“ping+空格+IP 地址”，如 ping 192.168.0.15，如下图所示。



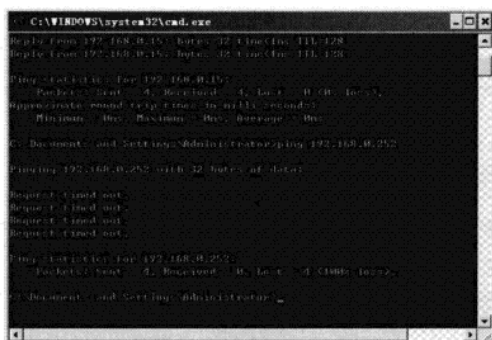
STEP 04 查看测试结果，网络连通

按【Enter】键，如果显示“Reply from……”表示两台计算机之间是连通的，如下图所示。



STEP 05 查看测试结果，网络中断

查看测试结果，如果显示 Request timed out，则说明两台计算机不能连通，如下图所示。



STEP 06 使用 " ping+空格+网站地址 " 格式

另外，还可以使用“ping+空格+网站地址”格式来测试本机与某个服务器的连通状态，如下图所示。



下面将介绍 ping 命令的几个常用参数：
❖ -a: 解析计算机 NetBIOS 名。

Chapter 01 黑客基础知识

❖ **-n count**: 发送 count 指定的 Echo 数据包数。在默认情况下，一般都只发送四个数据包，通过这个命令可以自己定义发送的个数，这对衡量网络速度很有帮助。

❖ **-l size**: 定义 echo 数据包大小。在默认的情况下 Windows 的 ping 命令发送的数据包大小为 32 B，用户也可以自定义它的大小，但有一个大小的限制，最大只能发送 65 500 B，因为 Windows 系列的操作系统都有一个安全漏洞（也许还包括其他系统），就是当向对方一次发送的数据包大于或等于 65 532 B 时，对方就很有可能无法正常工作，所以微软公司为了解决这一安全漏洞而限制了 ping 的数据包大小。

❖ **-f**: 在数据包中发送“不要分段”标志。一般发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再进行分段处理。

❖ **-v TOS**: 将“服务类型”字段设置为 tos 指定的值。

❖ **-i TTL**: 指定 TTL 值在对方的系统里停留的时间。此参数同样是帮助检查网络的运转情况。

❖ **-r count**: 在“记录路由”字段中记录传出和返回数据包的路由。在一般情况下发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定想探测经过的路由的个数，不过限制在了 9 个，也就是说只能跟踪到 9 个路由，如果想探测更多，可以通过其他命令实现。

❖ **-s count**: 指定 count 指定的跃点数的时间戳。此参数和 -r 差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录 4 个。

❖ **-j host-list**: 利用 computer-list 指定计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

❖ **-k host-list**: 利用 computer-list 指定计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

❖ **-w timeout**: 指定超时时间，单位为“毫秒”。

❖ **-t**: 连续对 IP 地址执行 ping 命令，直到被用户按【Ctrl+C】组合键中断。

1.4.2 net 命令

net 命令是一个功能强大、以命令行方式执行的命令，它包含了管理网络环境、服务、用户、登录等 Windows 98/NT/2000 中大部分重要的管理功能。使用它可以轻松地管理本地或者远程计算机的网络环境以及各种服务程序的运行和配置，或者进行用户管理和登录管理等。

下面将结合实例对 net 命令的不同参数的基本应用做一些初步的介绍，希望能对用户学习 net 命令有所帮助。

Work1 net localgroup 命令

该命令用于添加、显示或更改本地组，其命令格式为：

net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]

如果输入不带参数的 net localgroup 命令，将显示服务器名称和计算机的本地组名称；groupname 是要添加、扩充或删除的本地组名称，只提供 groupname 即可查看用户列表或本地组中的全局组；/comment: "text" 用来为新建或现有组添加注释，注释文字的最大长度是

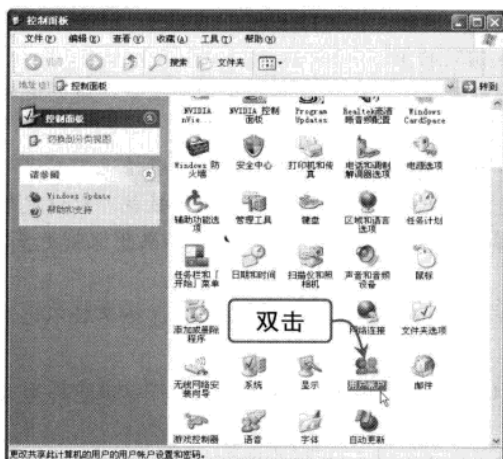


48 个字符，并用引号引住；/domain 在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作；/add 将全局组名或用户名添加到本地组中，在使用该命令将用户或全局组添加到本地组之前，必须为其建立账号；/delete 从本地组中删除组名或用户名。

下面以将受限用户 guo 加入本子管理员组为例，介绍 net localgroup 命令的使用方法：

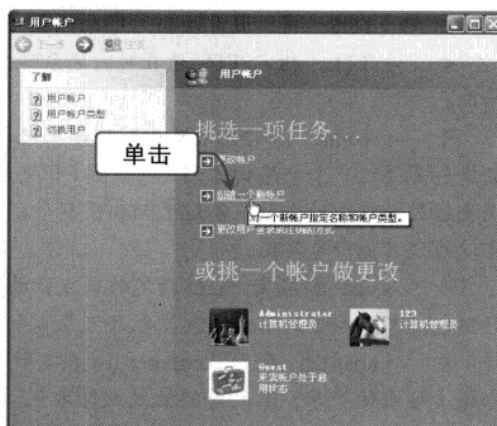
STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“用户账户”图标，如下图所示。



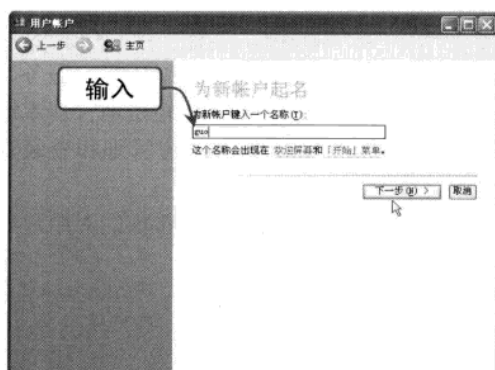
STEP 02 创建新账户

在“用户账户”窗口中单击“创建一个新账户”超链接，如下图所示。



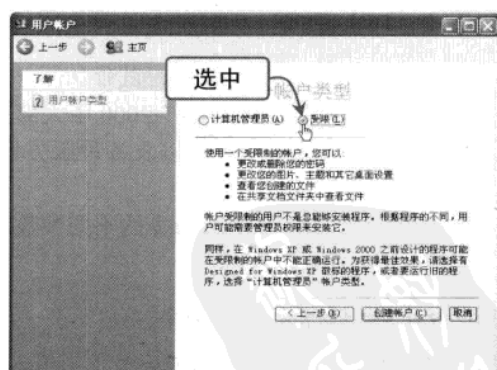
STEP 03 输入账户名称

弹出“为新账户起名”窗口，在“为新账户键入一个名称”文本框中输入新账户名称 guo，如下图所示。



STEP 04 选中“受限”单选按钮

单击“下一步”按钮，在“挑选一个账户类型”窗口中选中“受限”单选按钮，如下图所示。



STEP 05 创建受限账户

单击“创建账户”按钮，即可创建一个受限账户，如下图所示。

STEP 06 执行 net localgroup 命令

打开“命令提示符”窗口，执行命令 net localgroup administrators guo /add，即可将受限用户添加到系统的管理员账户中，如下图所示。

Chapter 01 黑客基础知识

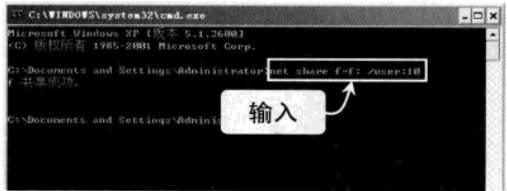


Work2 net share 命令

该命令用于创建、删除或显示共享资源，其命令格式为：
net share sharename
或
net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]
或
net share sharename [/users:number | unlimited] [/remark:"text"]
或
net share {sharename | drive:path} /delete
当输入不带参数的 net share 命令时，将显示本地计算机上所有共享资源的信息；sharename 是共享资源的网络名称，输入带 sharename 的 net share 命令，只显示该共享信息；drive:path 是指定共享目录的绝对路径；/users:number 用于设置可同时访问共享资源的最大用户数；/unlimited 为不限制同时访问共享资源的用户数；/remark:"text"用于添加关于资源的注释，注释文字用引号引住；/delete 为停止共享资源。
下面以共享本地磁盘 F 为例，详细介绍 net share 命令的使用方法：

STEP 01 共享本地磁盘 F

在“命令提示符”窗口中输入命令“net share f=f:/user:10”，按【Enter】键即可共享本地磁盘 F，如下图所示。



STEP 02 取消本地磁盘 F 的共享

要取消本地磁盘 F 的共享，可以在“命令提示符”窗口中输入命令 net share f/delete，然后按【Enter】键执行命令，如下图所示。



Work3 net user 命令

该命令用于添加或更改用户账号或显示用户账号信息，其命令格式为：
net user [username [password | *] [options]] [/domain]

黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码防
电子邮
件攻防
C 盘病
使用电
脑安全
黑客攻
防技巧



或

```
net user username {password | *} /add [options] [/domain]
```

或

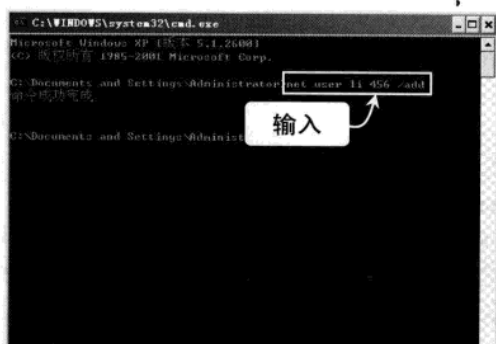
```
net user username [/delete] [/domain]
```

如果输入不带参数的 `net user` 命令将查看计算机上的用户账号列表；`username` 为添加、删除、更改或查看用户账号名，用户账号名最多可以有 20 个字符；`password` 为用户账号分配或更改密码，密码必须满足在 `net accounts` 命令/`minpwlen` 选项中设置的最小参数（此命令可参考相关资料，本书限于篇幅不做详细介绍）。“*”提示输入密码，在密码提示行中输入密码时，将不显示该密码；`/domain` 在计算机主域的主域控制器中执行操作，该参数仅在 Windows NT Server 域成员的 Windows NT Workstation 计算机上可用；`/add` 将用户账号添加到用户账号数据库；`/delete` 从用户账号数据库中删除用户账号。

下面以创建一个名为 `li` 的受限账户，然后将其删除为例，详细介绍 `net user` 命令的使用方法：

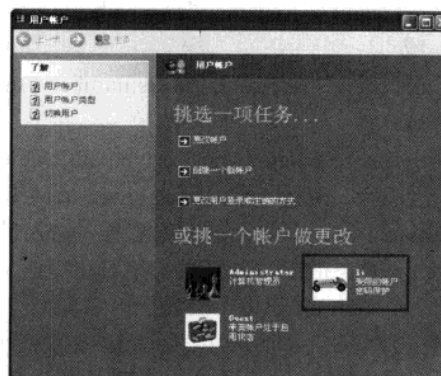
STEP 01 输入添加账户命令

打开“命令提示符”窗口，输入 `net user li 456 /add` 命令，然后按【Enter】键执行命令，如下图所示。



STEP 02 创建受限账户

此时在“用户账户”窗口中将创建一个名为 `li`、密码为 456 的受限账户，如下图所示。



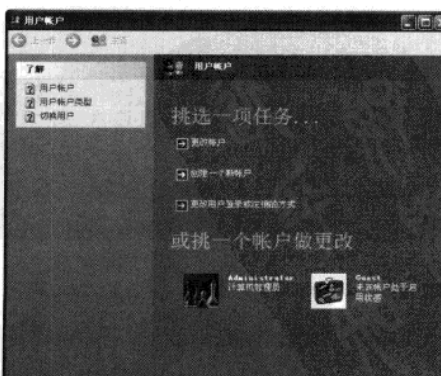
STEP 03 输入删除账户命令

在“命令提示符”窗口中，输入命令 `net user li /delete`，然后按【Enter】键执行命令，如下图所示。



STEP 04 删除受限账户

此时在“用户账户”窗口中将删除刚刚创建的受限账户 `li`，如下图所示。



Chapter 01 黑客基础知识

Work4 net view 命令

该命令用于显示域列表、计算机列表或指定计算机的共享资源列表，其命令格式为：

net view [\computername | /domain [:domainname]]

或

net view /network:nw [\computername]

如果输入不带参数的 net view 命令将显示当前域的计算机列表；\computername 指定要查看其共享资源的计算机；/domain [:domainname]指定要查看其可用计算机的域，如果省略 domainname，则显示网络的所有域；/network:nw 显示 NetWare 网络中所有可用的服务器；如果指定计算机名，则显示 NetWare 网络中该计算机的可用资源。

利用 net view 命令查看当前域中的共享资源的具体操作方法如下：

STEP 01 查看当前域中的计算机列表

打开“命令提示符”窗口，输入 net view 命令，然后按【Enter】键执行命令，即可显示当前域中的计算机列表，如下图所示。



STEP 02 查看某台计算机的共享资源

在“命令提示符”窗口中输入命令 net view \\c251，即可查看域中名为 c251 的计算机的共享资源，如下图所示。



提示

如果不知道对方的计算机名，可以直接输入对方的 IP 地址，如输入命令 net view \\192.168.0.251，然后按【Enter】键同样可以查看该计算机的共享资源。

1.4.3 netstat 命令

netstat 命令是一个监控 TCP/IP 网络的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息，用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。该命令的格式为：

netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

-a 显示所有的有效连接信息列表，包括已建立的连接和那些监听连接请求的连接；-e 用于显示关于以太网的统计数据，它列出的项目包括传送数据包的总字节数、错误数、删除数、数据报的数量和广播的数量；-n 显示所有已建立的有效连接；-r 显示关于路由表的信息，除了显示有效路由外，还显示当前有效的连接；-s 按照各个协议分别显示其统计数据。

- 常用扫描
- 与嗅探工具
- 统漏洞攻防
- 设置系统
- 安全策略
- 系统与文
- 件加密
- 远程控
- 木马
- 聊天软
- 网页恶
- 电子邮
- C盘病
- 使用电
- 黑客攻



下面将简单介绍 netstat 命令的使用方法：

STEP 01 显示所有连接和监听端口

打开“命令提示符”窗口，输入命令 netstat -a，然后按【Enter】键执行命令，即可显示所有连接和监听窗口，如下图所示。



STEP 02 显示路由表

在“命令提示符”窗口中，输入 netstat -r 命令，按【Enter】键执行命令，即可显示路由表，如下图所示。



1.4.4 ftp 命令

ftp 命令使用“文件传送协议”（FTP）在本地和远程主机或远程主机之间传送文件，利用此命令我们可以执行文件下载、上传、查看文件信息等操作。该命令的格式为：

ftp [-d] [-g] [-i] [-n] [-v] [-f] [-k realm] [-q[-C]] [HostName [Port]]

-d 使用调试方式；-g 取消全局文件名；-i 传送多个文件时关闭交互操作；-n 限制 FTP 的自动登录，即不使用 netre 文件；-v 显示远程服务器的所有响应信息。

下面通过一个已经设置好的 FTP 服务器为例，详细介绍利用 ftp 命令上传文件的方法：

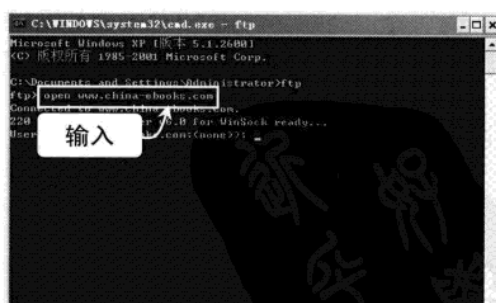
STEP 01 进入 ftp 命令模式

打开“命令提示符”窗口，在该窗口中输入命令 ftp，按【Enter】键进入 ftp 命令模式，如下图所示。



STEP 02 输入 FTP 服务器地址

输入 FTP 服务器的地址，在这里用的命令为 open www.china-ebooks.com，如下图所示。



STEP 03 输入用户名

根据屏幕提示输入用户名信息，这里输入的命令为 joyart，如下图所示。

STEP 04 输入登录密码

根据屏幕提示，在 Password 后输入登录密码，在这里密码是不显示的，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 01 黑客基础知识

基础
知识

与嗅探工具

常用扫描

系统漏洞攻防

安全策略

设置系统

系统安全

远程控制

木马

网页

代码

攻击

防御

安全

应用

黑
客
基
础
知
识

STEP 05 查看服务器上的文件信息

屏幕显示 xxx user logged in, 表明登录成功, 输入命令 dir, 查看服务器上的文件和文件夹信息, 如下图所示。

STEP 06 定位上传文件的本地磁盘位置

输入命令 lcd f:\, 按【Enter】键执行命令, 定位到要上传文件的本地磁盘位置 F 盘, 如下图所示。

STEP 07 上传文件

输入命令 put ceshi.txt, 按【Enter】键执行命令, 即可将本地磁盘 F 下的 ceshi.txt 文件上传到 FTP 服务器上, 如下图所示。

STEP 08 下载文件

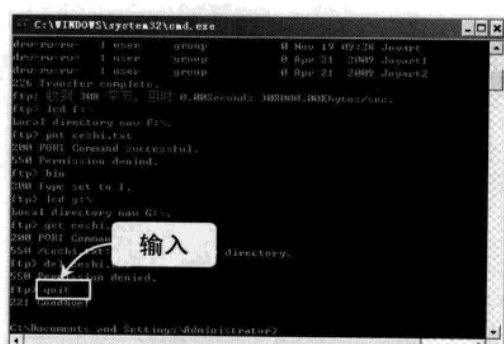
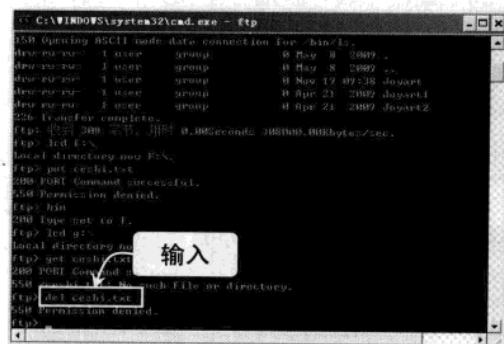
定位到要下载文件的保存位置, 然后输入命令 get ceshi.txt, 即可下载刚刚上传的文件, 如下图所示。

STEP 09 删除上传文件

输入命令 del ceshi.txt, 按【Enter】键执行, 即可将上传的文件删除, 如下图所示。

STEP 10 退出 FTP 服务器

输入命令 quit, 按【Enter】键执行, 即可退出 FTP 服务器, 如下图所示。



1.4.5 telnet 命令

telnet 命令允许用户使用 telnet 协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像在本地电脑上一样执行各种操作。该命令的格式为：

telnet [-a] [-e escape char] [-f log file] [-l user] [-t term] [host [port]]

-f 指定客户端登录的文件名；-l 指定远程系统上登录用的用户名；-t 指定终端类型；host 指定要连接的远程计算机的主机名或 IP 地址；port 指定端口号或服务名。

利用 telnet 命令远程登录的具体操作方法如下：

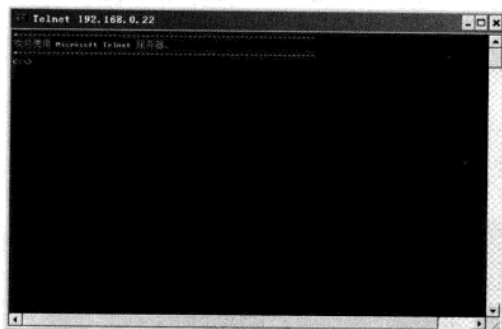
STEP 01 进入远程登录界面

打开“命令提示符”窗口，在该窗口中输入命令 telnet 192.168.0.22，按【Enter】键进入远程登录界面，如下图所示。



STEP 02 输入用户名和密码

输入 n 后按【Enter】键，然后在 login:后输入该计算机的用户名，再在 password: 后输入登录密码，确认后即可，如下图所示。



1.4.6 ipconfig 命令

ipconfig 命令用于显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的 ipconfig 命令可以显示所有适配器的 IP 地址、子网掩码和默认网关。该命令的格式为：

ipconfig [/all] [/renew [adapter] [/release[adapter] [/flushdns] [/displaydns] [/registerdns] [/showclassid adapter] [/setclassid adapter [classID]]

使用不带参数的 ipconfig 命令可以显示所有适配器的 IP 地址、子网掩码和默认网关；/all

Chapter 01 黑客基础知识

显示所有适配器的完整 TCP/IP 配置信息；/renew [adapter]更新所有适配器或特定适配器的 DHCP 配置信息；/release [adapter]发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器或特定适配器的当前 DHCP 配置并丢弃 IP 地址配置；/flushdns 清理并重设 DNS 客户解析器缓存的内容；/displaydns 显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录。

利用 ipconfig 命令查看本地适配器的 TCP/IP 信息的方法如下：

STEP 01 查看 IP 地址和默认网关

打开“命令提示符”窗口，在该窗口中输入命令 ipconfig，按【Enter】键执行，即可查看本地计算机的 IP 地址、子网掩码和默认网关，如下图所示。



STEP 02 查看完整 TCP/IP 配置信息

输入命令 ipconfig /all 后按【Enter】键，即可在“命令提示符”窗口中查看本地计算机的完整 TCP/IP 配置信息，如下图所示。



提示

ipconfig 是调试计算机网络的常用命令，通常用户使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。其实这只是 ipconfig 的不带参数用法，而它的带参数用法在网络应用中也是相当不错的。

1.5 创建安全的测试环境

为了学习黑客知识，常常需要在自己的电脑上安装一些木马或黑客程序进行测试，为了保障系统安全，用户可以在当前系统上安装虚拟机，构建一个虚拟测试环境，这样既可以保障系统安全，又可以方便地学习黑客操作知识。

1.5.1 安装 VMware 虚拟机

下面以 VMware 7.0 为例，详细介绍安装 VMware 虚拟机的操作步骤：

STEP 01 运行软件安装程序

双击 VMware 7.0 安装程序图标，开始运行安装程序，如下图所示。

STEP 02 选择安装方式

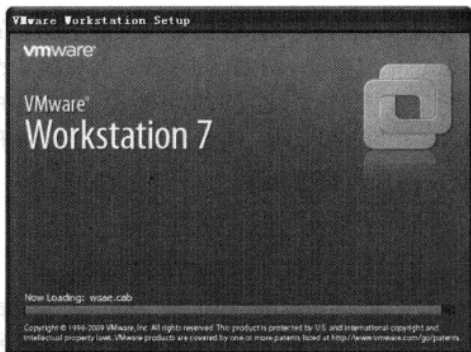
在开始安装界面单击 Next 按钮，在如下图所示的界面中选择安装方式，这里单击 Custom 按钮。

黑客
基础知识
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
安全策略
设置系统
件加密
系统与文
件加解密
远程控制
制攻防
木马
攻防
聊天软
件攻防
网页恶意
代码攻防
件攻防
电子邮箱
C 盘病毒
使用电脑
安全软件
黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

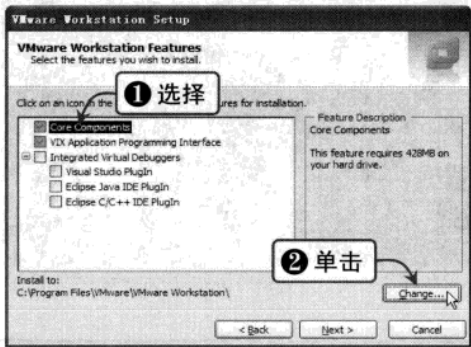


黑客攻防从新手到高手



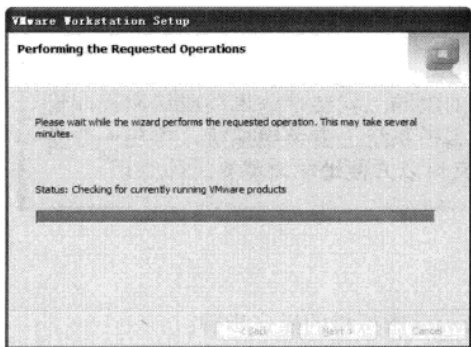
STEP 03 选择要安装的程序

在如下图所示的界面中选择要安装的程序，然后单击 Change 按钮，设置安装路径。



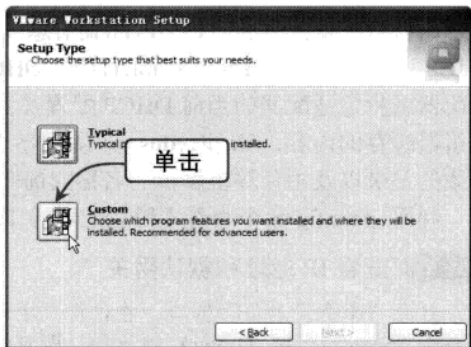
STEP 05 开始安装文件

在弹出的界面中单击 Continue 按钮，开始按照上述设置安装文件，如下图所示。



STEP 07 重新启动系统

在如下图所示的界面中单击 Restart Now 按钮，重新启动系统。



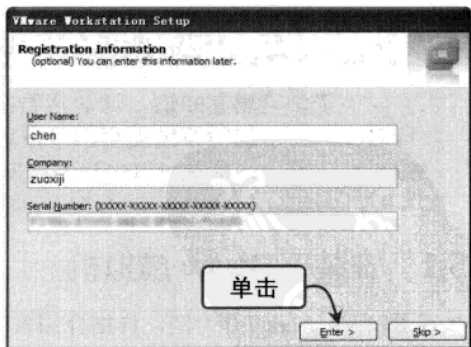
STEP 04 直接单击 Next 按钮

单击“确定”按钮返回，继续单击 Next 按钮，在如下图所示的界面中直接单击 Next 按钮。



STEP 06 选择安装位置

文件安装完毕后，将弹出如下图所示的界面，输入用户名、公司名和软件序列号，然后单击 Enter 按钮继续。



STEP 08 运行 VMware 虚拟机


系统启动后，双击桌面上的 VMware Workstation 图标，运行 VMware 虚拟机，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 01 黑客基础知识

STEP 09 打开 VMware 虚拟机主界面

选中 “Yes, I accept the terms in the license agreement” 单选按钮，然后单击 OK 按钮，即可打开 VMware 虚拟机主界面，如右图所示。



提示

VMware 的安装方法与其他软件相似，用户根据屏幕提示进行操作即可。

STEP 02 选择安装方式

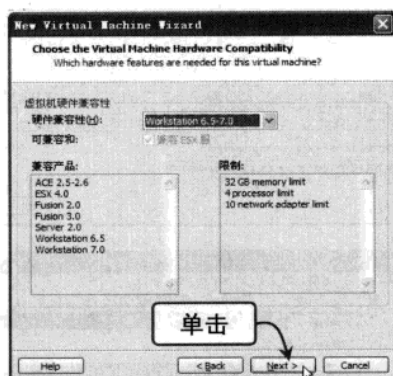
弹出 “欢迎来到新建虚拟机向导” 界面，选中 “自定义（高级）” 单选按钮，然后单击 Next 按钮，如下图所示。

基础知
黑客
常用扫描
与嗅探工具
系统漏洞攻防
安全策略
设置系统
系统安全
加密
远程控制
木马
聊天软
网页恶意
代码攻防
件攻防
件攻防
毒攻防
安全软件
使用电脑
黑客攻防
实用技巧



STEP 03 设置虚拟机的硬件兼容性

在弹出的界面中设置虚拟机的硬件兼容性，这里保存系统默认设置，直接单击 Next 按钮，如下图所示。



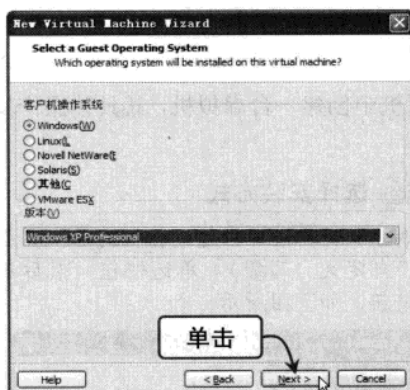
STEP 04 设置操作系统安装文件的来源

在弹出的界面中设置操作系统安装文件的来源，这里选中“我将操作系统以后安装”单选按钮，如下图所示。



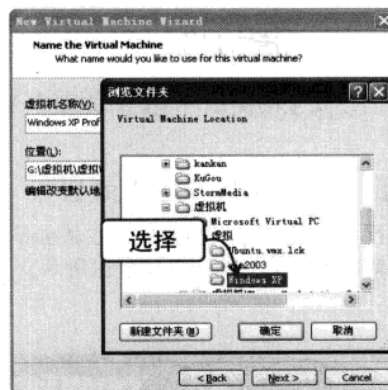
STEP 05 设置客户机操作系统的类型

单击 Next 按钮，在弹出的界面中设置客户机操作系统的类型，这里选中 Windows 单选按钮，并在下方的“版本”下拉列表框中选择 Windows XP Professional 选项，如下图所示。



STEP 06 为创建的虚拟机命名

单击 Next 按钮，在弹出的界面中为创建的虚拟机命名，这里在“虚拟机名称”文本框中输入 Windows XP Professional，然后单击“浏览”按钮，在弹出的“浏览文件夹”中选择虚拟机安装位置，如下图所示。



提示

在设置客户机操作系统类型时，用户既可以选择安装 Windows 系列的 Windows XP 或 Windows Server 2003，也可以选择安装 Linux、Novell NetWare 或 Solaris 操作系统。

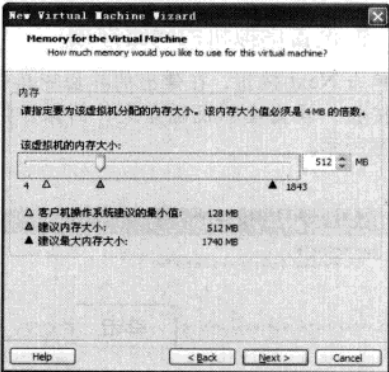
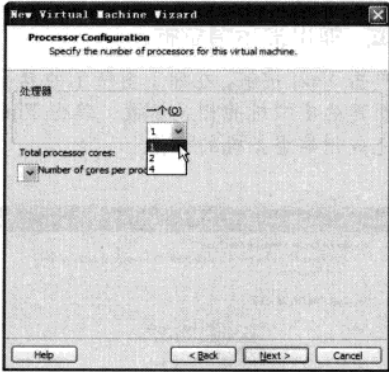
STEP 07 选择处理器的数量

单击 Next 按钮，在弹出的界面中选择处理器的数量，如下图所示。

STEP 08 设置虚拟机的内存大小

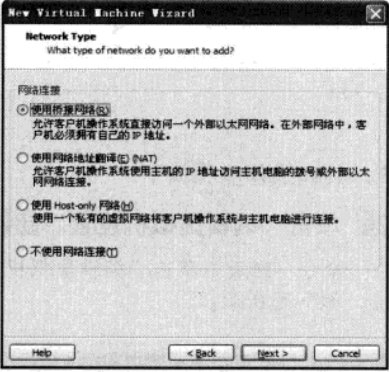
单击 Next 按钮，在弹出的界面中设置虚拟机的内存大小，如下图所示。

Chapter 01 黑客基础知识



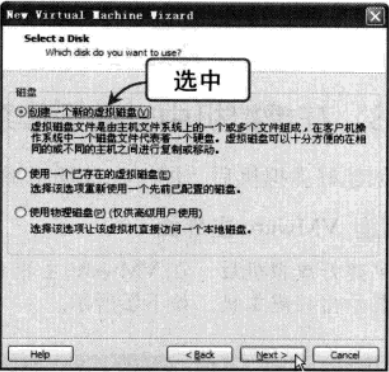
STEP 09 设置虚拟机的网络连接

单击 Next 按钮，在弹出的界面中设置虚拟机的网络连接，这里选中“使用桥接网络”单选按钮，如下图所示。



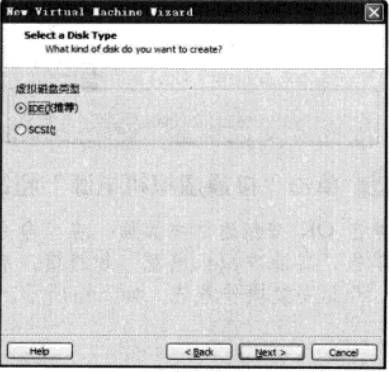
STEP 10 创建一个新的虚拟磁盘

依次单击 Next 按钮，在如下图所示的界面中选中“创建一个新的虚拟磁盘”单选按钮。



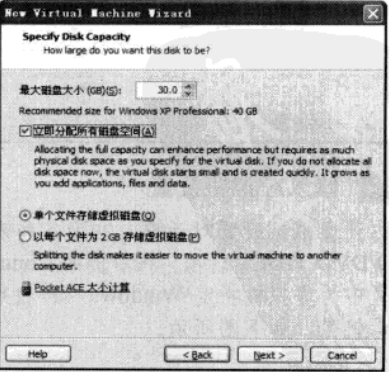
STEP 11 设置虚拟磁盘类型

单击 Next 按钮，在弹出的界面中设置虚拟磁盘类型，这里选中“IDE（推荐）”单选按钮，如下图所示。



STEP 12 设置最大磁盘大小

单击 Next 按钮，在如下图所示的界面中设置最大磁盘大小，并选中“立即分配所有磁盘空间”复选框。

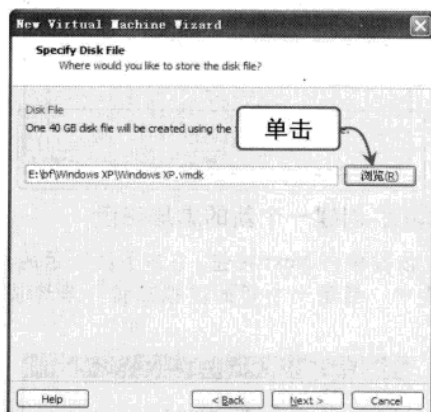


基础知识
与嗅探工具
统漏洞攻防
安全策略
系统安全
加密解密
远程控制
木马攻击
聊天软件
网页恶意
代码攻防
电子取证
C++攻防
安全软件
黑客攻防
实用技巧



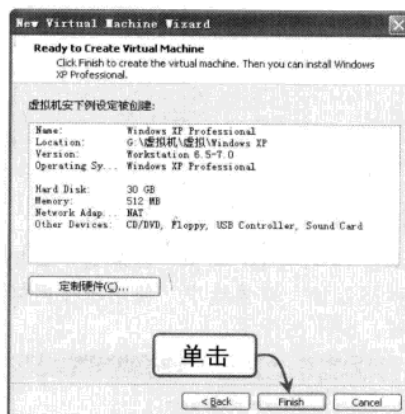
STEP 13 设置虚拟机的网络连接

单击 Next 按钮，在弹出的界面中单击“浏览”按钮，设置虚拟机磁盘文件的保存位置，如下图所示。



STEP 14 弹出提示信息框

单击 Next 按钮，在如下图所示的界面中显示新建的虚拟机的相关参数，单击 Finish 按钮，完成创建虚拟机的操作。

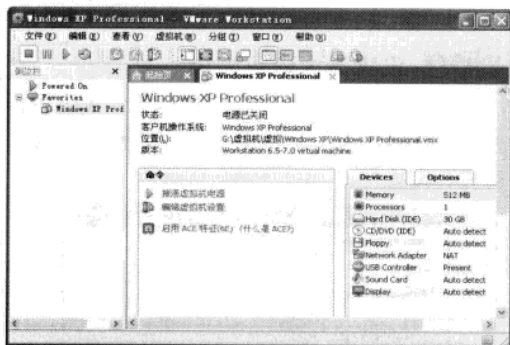


1.5.3 在虚拟机中安装操作系统

创建好虚拟机后，即可在此环境下安装操作系统，具体操作步骤如下：

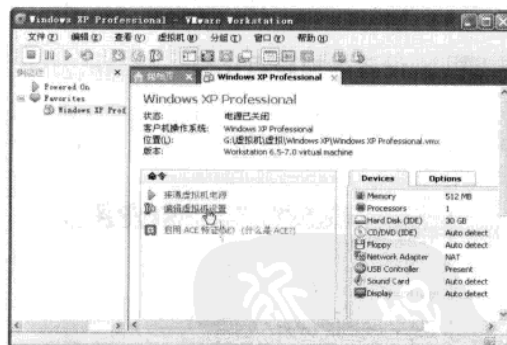
STEP 01 VMware 主界面

创建好虚拟机后，在 VMware 主界面中将自动显示出该虚拟机，如下图所示。



STEP 02 单击“编辑虚拟机设置”超链接

在“命令”列表中单击“编辑虚拟机设置”超链接，如下图所示。



STEP 03 修改虚拟机设置

打开虚拟机设置对话框，在设备列表中选择 CD/DVD (IDE) 选项，在右侧的 Connection 选项区中为虚拟机指定 Windows XP 的系统安装文件镜像，如下图所示。

STEP 04 单击“接通虚拟机电源”超链接

单击 OK 按钮返回主界面，在“命令”列表中单击“接通虚拟机电源”超链接，启动虚拟机，开始安装操作系统，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 01 黑客基础知识



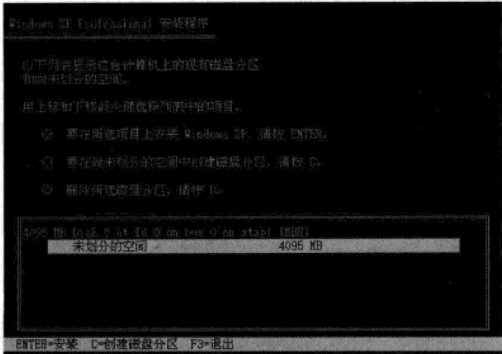
STEP 05 虚拟机开始启动

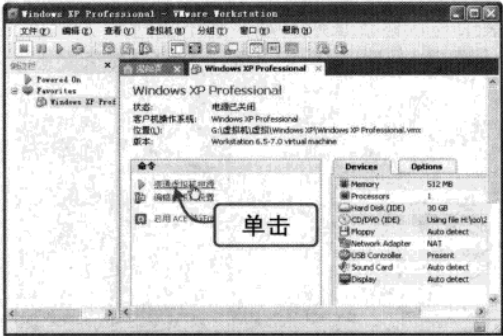
创建的 Windows XP 虚拟机开始启动，如下图所示。



STEP 07 创建磁盘分区


检测系统硬件设备后，按【Enter】键继续，在如下图所示的界面中创建磁盘分区。





STEP 06 进入系统安装界面

稍后虚拟机开始运行虚拟镜像上的 Windows XP 安装文件，进入系统安装界面，如下图所示。



STEP 08 格式化分区

根据屏幕提示，创建好磁盘分区后对其进行格式化操作，如下图所示。

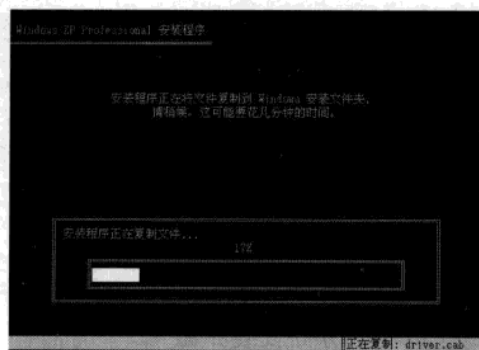


黑客基础知识
常用扫描与嗅探工具
Windows系统漏洞攻防
设置系统安全策略
系统与文件加密
远程控制攻防
木马攻防
聊天软件攻防
网页恶意代码攻防
电子邮箱攻防
C盘病毒攻防
使用电脑安全软件
黑客攻防实用技巧



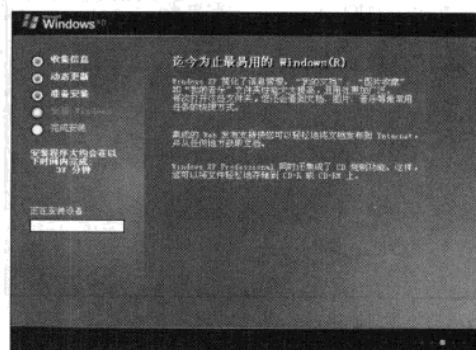
STEP 09 复制安装文件并重新启动

格式化完成后，系统开始自动复制系统安装文件，然后重新启动，如下图所示。



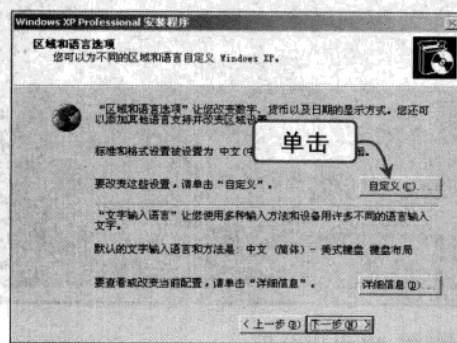
STEP 10 开始自动安装系统

重新启动后安装程序便会开始自动安装系统，如下图所示。



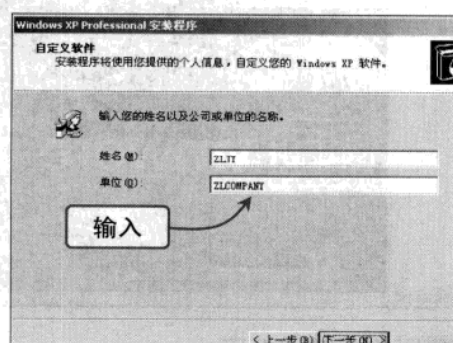
STEP 11 改变系统区域和语言设置

在“区域和语言选项”界面中单击“自定义”按钮，可以改变系统区域和语言设置，如下图所示。



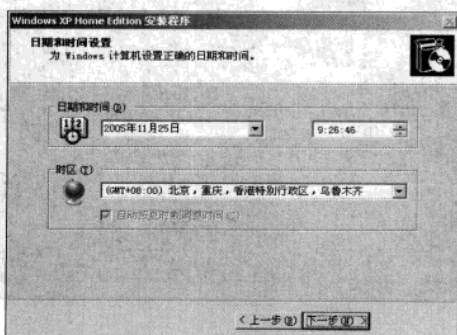
STEP 12 输入姓名和单位信息

在“自定义软件”界面的文本框中分别输入姓名和单位信息，如下图所示。



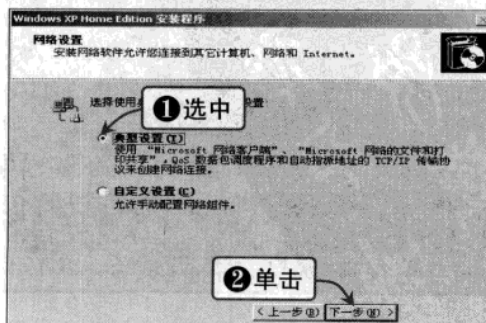
STEP 13 修改系统日期和时间设置

在“日期和时间设置”界面中可以修改系统日期和时间设置，如下图所示。



STEP 14 选中“典型设置”单选按钮

在“网络设置”界面中选中“典型设置”单选按钮，然后单击“下一步”按钮继续，如下图所示。

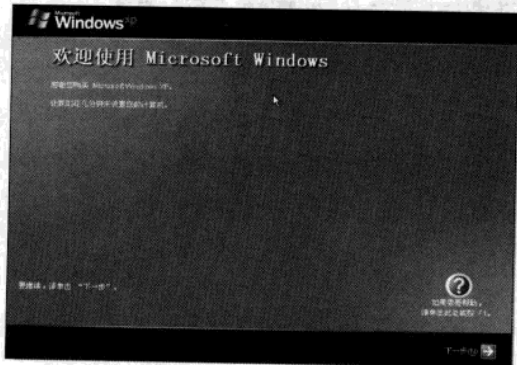


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 01 黑客基础知识

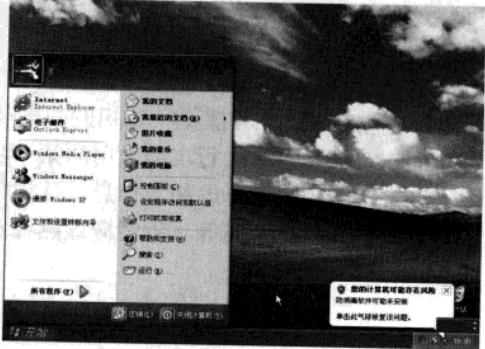
STEP 15 完成安装工作

安装程序自动完成剩余的安装工作后，电脑再次重新启动，进入 Windows XP 的欢迎界面，如下图所示。



STEP 16 登录系统

根据屏幕提示进行相应设置后，即可登录到 Windows XP 的系统桌面，如下图所示，完成在虚拟机中安装操作系统的操作。



● 读书笔记

Blank lined area for taking notes, with a small illustration of a notepad and pen in the bottom right corner.

- 基础知识
- 与嗅探工具
- 统漏洞攻防
- 安全策略
- 系统与安全
- 件加密
- 制攻防
- 攻防
- 件攻防
- 代码攻防
- 件攻防
- 毒攻防
- 安全软件
- 黑客攻防

Chapter

02

常用扫描与嗅探工具

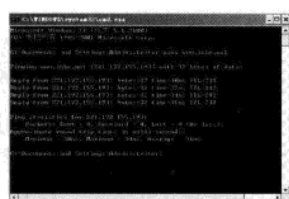
要想成为一名黑客，常用的扫描与嗅探工具当然是不可缺少的，网络扫描与嗅探是黑客进行攻击之前的第一步，也是必备的操作武器。本章将引领读者了解扫描目标的相关信息，认识常见端口扫描器、常见多功能扫描器、常用网络嗅探工具等，读者应该熟练掌握。

本章建议学习时间：

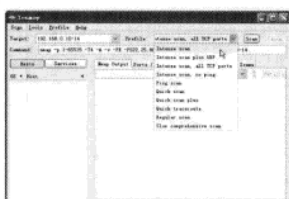
本章建议学习时间为 50 分钟，其中 10 分钟学习如何了解目标的相关信息，40 分钟学习认识常见端口扫描器、常见多功能扫描器、常用网络嗅探工具等知识。

学完本章后您可以：

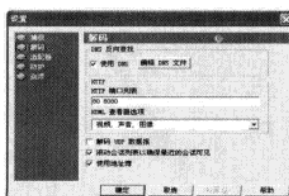
- 了解扫描目标的信息
- 认识扫描器
- 常见端口扫描器
- 常见多功能扫描器
- 常见专项功能扫描器
- 常用网络嗅探工具



利用 ping 命令



设置网络扫描方式



设置解码选项

重要知识点视频索引



Chapter 02 常用扫描与嗅探工具

2.1 了解扫描目标的相关信息

黑客在对一个攻击目标进行入侵和攻击之前，必须提前对这个目标的相关信息进行搜索和分析，找出系统漏洞，从而制订出最有效的入侵方案。

2.1.1 确定目标的 IP 地址

要对某个网络目标进行入侵，首先要知道这个目标的“地址”，也就是它的 IP 地址。要确定目标的 IP 地址很简单，通过如下方法即可实现：

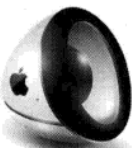
STEP 01 利用 ping 命令

在“命令提示符”窗口中输入命令 ping www.inhe.net，按【Enter】键执行，即可看到银河网站的 IP 地址，如下图所示。



STEP 02 利用 nslookup 命令

在“命令提示符”窗口中输入命令 nslookup www.inhe.net，然后按【Enter】键，同样可以确定目标的 IP 地址，如下图所示。



提示

nslookup 是 Windows NT/2000 操作系统中用于连接 DNS 服务器、查询域名信息的一个非常有用的命令。该命令一直从前上下文中的名称中抽去后缀，如果无法进行完全合格的名称查询，那么查询将被附加到当前上下文中。

2.1.2 查看目标所属地区

获得目标的 IP 地址后，就可以通过查询 IP 地址数据库来查看目标的所属地区。现在很多网站都提供 IP 地址查询服务，利用此项服务我们可以轻松查找到此 IP 地址所属地区及其相关信息。下面以百度搜索引擎中的 IP 地址查询服务为例，介绍利用 IP 查看目标所属地区的方法。

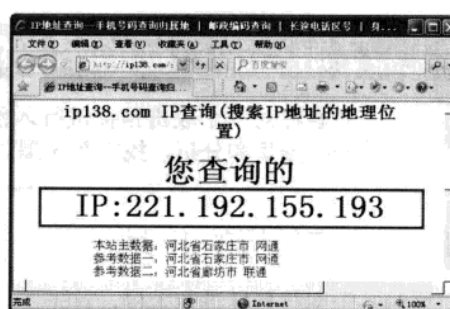
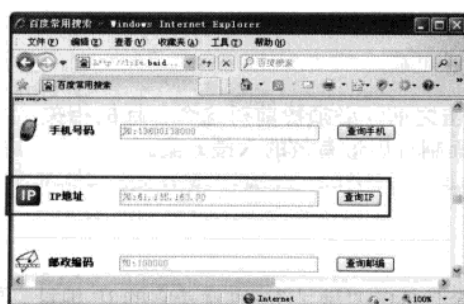
STEP 01 打开 IP 地址查询服务网页

在百度网站首页中单击“更多”超链接，在弹出的页面中单击“常用搜索”超链接，打开“百度常用搜索”页面，在该页面中找到“IP 地址”查询区域，如下图所示。

STEP 02 查看 IP 地址所属地区

在“IP 地址”右侧的文本框中输入要查询的 IP 地址，这里以上例获得的 IP 地址“221.192.155.193”为例，然后单击“查询 IP”按钮，在打开的页面中即可查看 IP 地址所属地区，如下图所示。

基础入门
黑客入门
常用扫描工具
Windows 系统漏洞攻防
设置系统安全策略
系统加密与解密
远程控制与木马
聊天软件攻防
网页恶意代码攻防
电子邮箱攻防
C 盘病毒使用电脑安全软件
黑客攻防技巧



2.2 认识扫描器

扫描器是一种自动检测远程或本地主机安全漏洞的程序，通过使用扫描器可以不留痕迹地发现远程服务器的各种 TCP 端口的分配、提供的服务和它们的软件版本，这些信息可以让我们直接或间接了解主机所存在的安全问题。

2.2.1 扫描器的工作原理

扫描器采用模拟攻击的形式对工作站、服务器、交换机、数据库应用等各种扫描对象可能存在的已知安全漏洞进行逐项检查，然后根据扫描结果向系统管理员提供安全性分析报告，为提高网络安全水平提供重要依据。

扫描器通常具有三项功能：发现一台主机和网络的能力；发现哪些服务正运行在当前这台主机上的能力；通过测试这些服务，发现当前主机存在的漏洞的能力。

在这里我们需要指出，扫描器并不是一个直接的攻击系统漏洞的程序，它仅仅能够帮助我们发现目标主机存在的某些弱点。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞，但它不会提供进入一个系统的详细步骤。

2.2.2 扫描器的作用

扫描器对 Internet 安全很重要，因为它能够快速查找到网络的脆弱点。我们都知道，在当前任何一个操作系统中都有很多我们所熟知的系统漏洞和设计缺陷，而这往往成为黑客入侵的一种便利途径。在大多数情况下，这些脆弱点都是唯一的，仅影响一个网络服务。人工测试单台主机的脆弱点是一项极其烦琐的工作，而扫描程序能轻易地解决这些问题。扫描程序开发者利用可得到的常用攻击方法并把它们集成到整个扫描中，这样使用者就可以通过分析输出的结果发现系统的漏洞。

在网络安全体系的建设中，网络扫描工具花费低、效果好、见效快，其安装运行简单，可以大规模减少安全管理员的手工劳动，有利于保持整个网络的安全和稳定。



提示

扫描器并不是一个直接的攻击网络漏洞的程序，它仅仅能帮助我们发现目标主机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标主机的漏洞，但它不会提供进入一个系统的详细步骤。

Chapter 02 常用扫描与嗅探工具

2.3 常见端口扫描器

服务器上所开放的端口往往是黑客潜在的入侵通道，对目标主机进行端口扫描能够获得许多有用的信息，而进行端口扫描的方法也很多，可以是手工进行扫描，也可以用端口扫描软件进行，黑客常用的端口扫描器有 Nmap、SuperScan 等。

2.3.1 Nmap 扫描器

Nmap 是 Linux、FreeBSD、UNIX、Windows 系统环境下的网络扫描和嗅探工具，它的基本功能有三个：探测一组主机是否在线；扫描目标主机端口，查看主机所提供的网络服务；推断主机所用的操作系统。

Work1 Nmap 简介

Nmap 的设计目标是快速地扫描大型网络，它以新颖的方式使用原始 IP 报文来发现网络上有哪些主机、主机提供什么服务、哪些服务运行在什么操作系统上、它们使用什么类型的报文过滤器/防火墙等信息。它支持多种协议的扫描，如 udp、tcp connect()、tcp syn（半开）、ftp proxy（跳板攻击）、reverse-ident、icmp（ping）、fin、ack sweep、xmas tree、syn sweep 和 null 扫描。nmap 还提供一些实用功能，如通过 TCP/IP 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 ping 侦测下属的主机、欺骗扫描、端口过滤探测、直接的 rpc 扫描、分布扫描、灵活的目标选择以及端口的描述。

运行 Nmap 后通常会得到一个关于扫描的机器的一个实用的端口列表。Nmap 总是显示该服务的端口号、协议、服务名称以及状态，其状态有 open、filtered、closed 和 unfiltered 四种。open 指的是目标主机将会在该端口接收连接请求；filtered 指的是有防火墙或者其他过滤装置在这个端口进行过滤，所以 Nmap 需要进一步查明端口是否开放；closed 指当前端口是关闭的；unfiltered 状态只有在大多数的扫描端口都处在 filtered 状态下才会出现。

除了所感兴趣的端口表，Nmap 还能提供关于目标主机的进一步信息，包括反向域名、操作系统猜测、设备类型和 MAC 地址等。

Work2 Nmap 的安装

Nmap 原本是一个命令界面的扫描器，后来其官方网站又提供了带图形用户界面的版本，我们只需到 Nmap 的官方网站下载其 Windows 系统环境下的安装文件即可，下面将简单介绍其安装方法。

STEP 01 运行 Nmap 安装程序

在 Nmap 官方网站上找到其 Windows 系统环境下的安装文件，单击相应的下载链接进行下载，文件下载完毕后，双击其安装程序图标，运行 Nmap 安装程序，单击 I Agree 按钮，如下图所示。

STEP 02 保持默认设置

弹出安装选项界面，保持默认设置，直接单击 Next 按钮进行下一步安装，如下图所示。

基础知识

与嗅探工具

Windows 系统

设置系统

安全策略

系统与安全

远程攻击

木马

聊天软件

网页恶意

代码攻击

电子邮件

攻击

使用电脑

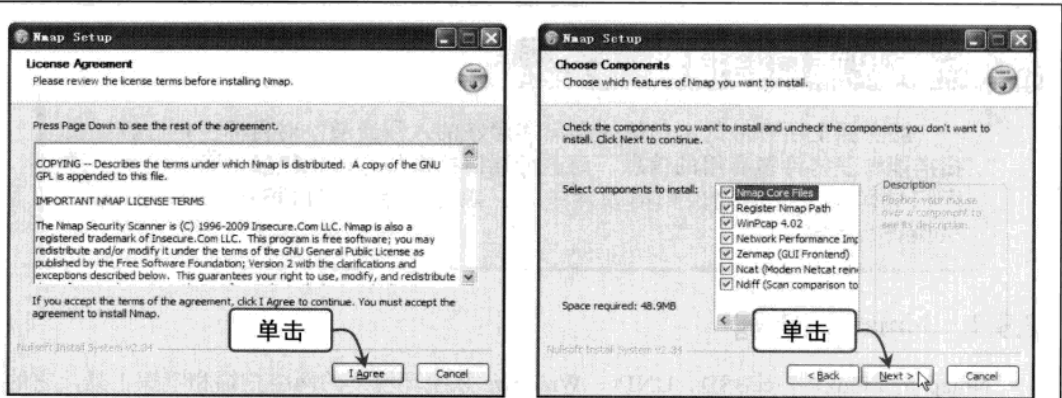
安全软件

黑客攻防

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

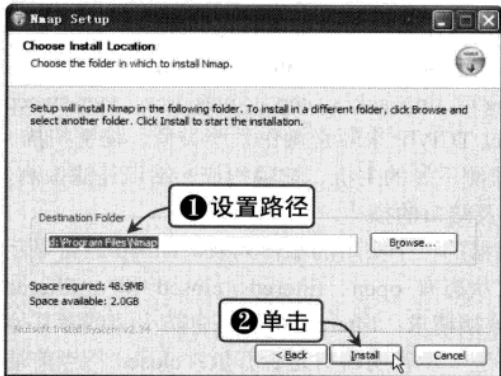


黑客攻防从新手到高手



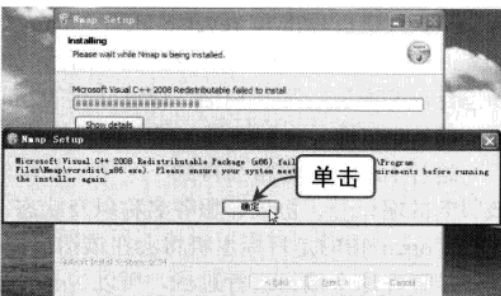
STEP 03 设置安装路径

在选择安装路径界面中，设置软件的安装路径，这里设置其路径为 d:\Program Files\Nmap，单击 Install 按钮开始安装，如下图所示。



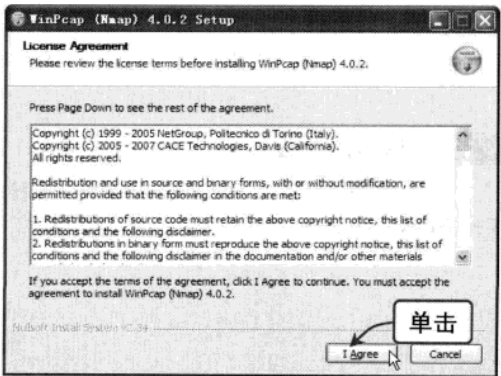
STEP 04 开始安装

在安装过程中可能会弹出提示信息，要求安装其他程序，根据屏幕提示单击相应按钮即可，如下图所示。



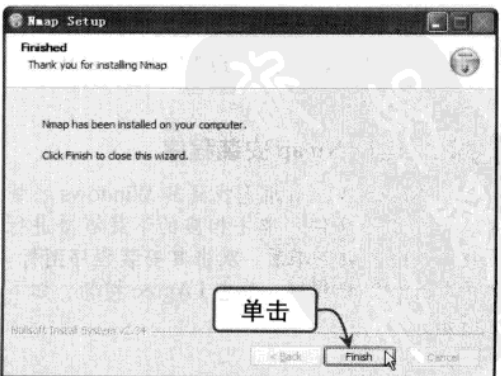
STEP 05 安装 WinPcap 程序

在安装过程中系统会提示用户安装 WinPcap 程序，根据屏幕提示单击相应的按钮进行安装，如下图所示。



STEP 06 完成程序安装

依次单击 Next 按钮继续安装，当出现完成界面时，单击 Finish 按钮即可完成安装，如下图所示。



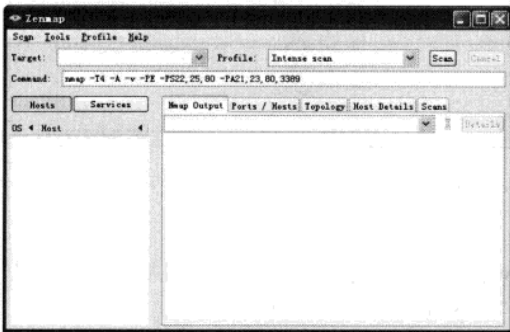
Chapter 02 常用扫描与嗅探工具

Work3 使用 Nmap 扫描

Nmap 包含多种扫描选项，它对网络中被检测到的主机按照选择的扫描选项和显示结点进行探查。我们可以建立一个需要扫描的范围，这样就不需要再输入大量的 IP 地址和主机名了。使用 Nmap 进行扫描的具体操作方法如下：

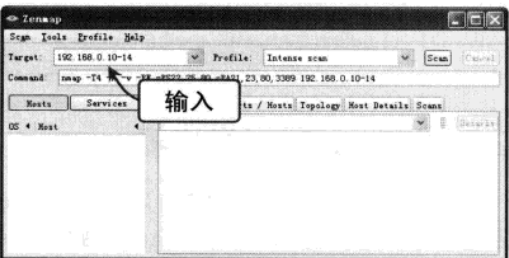
STEP 01 运行 Nmap 扫描程序

在桌面上双击 Nmap 程序图标，即可打开 Nmap 操作界面，如下图所示。



STEP 02 设置扫描范围

要扫描单台主机，可以在 Target 文本框内输入主机的 IP 地址或网址，要扫描某个范围内的主机，可以在该文本框中输入“192.168.0.10-14”，如下图所示。

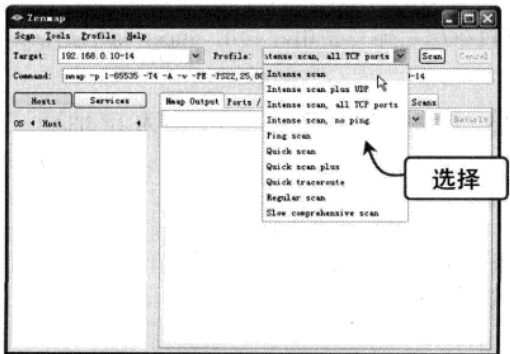


提示

在扫描时，还可以用“*”替换掉 IP 地址中的任何一部分，如“192.168.1.*”等同于“192.168.1.1-255”；要扫描一个更大范围内的主机，可以输入“192.168.1, 2, 3.*”，此时将扫描“192.168.1.0”、“192.168.2.0”、“192.168.3.0”三个网络中的所有地址。

STEP 03 设置网络扫描方式

要设置网络扫描的不同配置文件，可以单击 Profile 后的下拉列表框，从中选择 Intense scan、Intense scan plus UDP、Intense scan, all TCP ports 等选项，从而对网络主机进行不同方面的扫描，如下图所示。



STEP 04 查看扫描信息

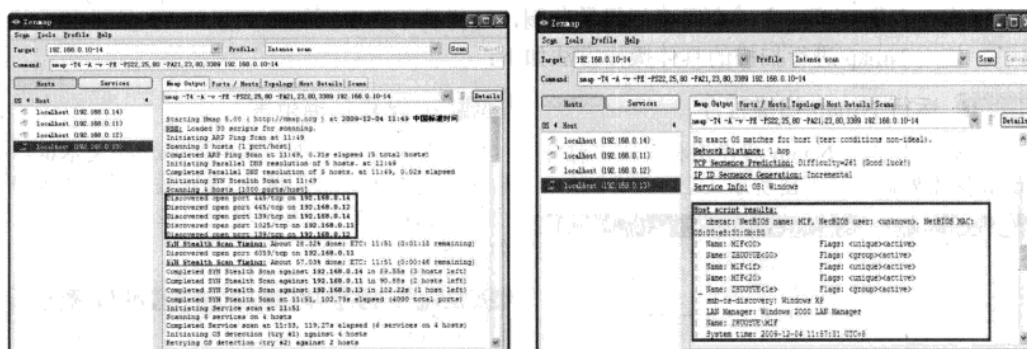
单击 Scan 按钮开始扫描，稍等一会儿，即可显示出扫描结果信息，如下图所示。



黑客
基础
知识
常用
扫描
与嗅
探工
具
Windows 系
统漏洞
攻防
设置系
统安全
策略
系统与
文
件加
密
远程
控制
木马
聊天
软件
网页
恶意
代码
攻击
电子
邮件
病毒
使用
电脑
安全
软件
黑客
技巧



在扫描结果信息中，可以看到扫描对象当前开放的端口，如下图（左）所示。
在扫描结果信息中，还可以了解扫描对象的系统信息，如下图（右）所示。



2.3.2 SuperScan 扫描器

SuperScan 是一款免费的、只运行于 Windows 平台之上的 TCP/UDP 端口扫描器，其中还包含许多其他网络工具，如 ping、路由跟踪、http head 和 whois 等。

Work1 SuperScan 的功能

对一个网络管理员或者网络攻击者而言，一款好的扫描软件是必不可少的，而 SuperScan 就是这样一款经典的 IP 和端口扫描软件，其主要功能如下：

- ❖ 通过 ping 命令来检验目标 IP 是否在线。
- ❖ IP 地址和域名相互转换。
- ❖ 检验目标主机提供的服务类别。
- ❖ 检验一定范围内的目标主机是否在线和端口情况。
- ❖ 自定义工具列表检验目标主机是否在线和端口情况。
- ❖ 自定义要检验的端口，并可以保存为端口列表文件。
- ❖ 软件自带一个木马端口列表 trojans.lst，通过这个列表用户可以检测目标主机是否有木马；同时，用户还可以自定义修改这个木马端口列表。

Work2 使用 SuperScan 扫描

SuperScan 是一款绿色软件，下载后将压缩包解压后即可使用。利用 SuperScan 扫描器进行扫描的具体操作步骤如下：

STEP 01 运行 SuperScan 扫描器

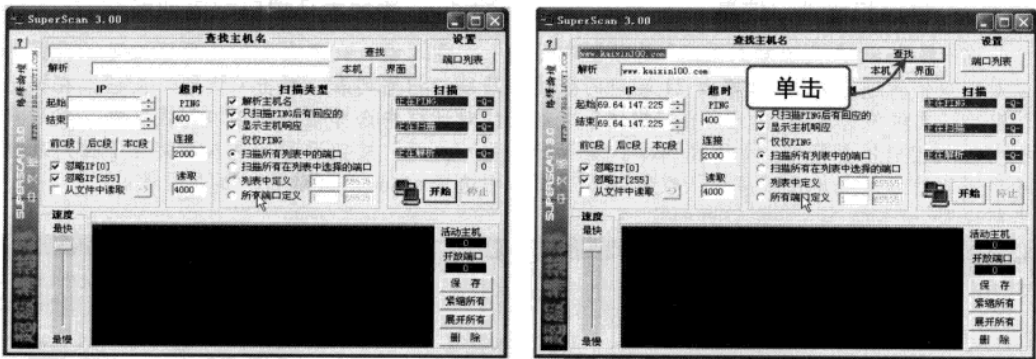
下载 SuperScan 扫描器后，将下载下来的压缩包解压，然后双击 SuperScan 扫描器图标，即可运行 SuperScan 扫描器，其工作界面如下图所示。

STEP 02 将扫描目标的域名转为 IP 地址

在“查找”按钮左侧的文本框中输入要扫描目标的域名，然后单击“查找”按钮，稍后即可找到扫描目标的 IP 地址，并且软件会自动将此 IP 地址添加到下面的“起始”和“结束”文本框中，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 02 常用扫描与嗅探工具

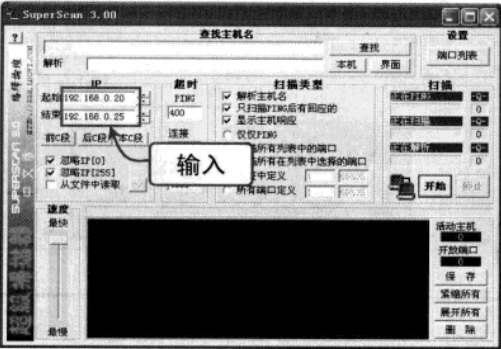


提示

如果要获得自己计算机的 IP 地址，可以单击“本机”按钮；要获取自己计算机的 IP 设置情况，可以单击“界面”按钮。

STEP 03 设置扫描范围

如果要扫描某一段范围内的多个主机，用户可以在“起始”文本框中输入起始 IP，在“结束”文本框中输入结束 IP。下图所示即为扫描“192.168.0.20-192.168.0.25”之间的所有主机。



提示

单击“前 C 段”按钮，可以直接转到前一个 C 网段；单击“后 C 段”按钮，可以直接转到后一个 C 网段；单击“本 C 段”按钮，可以直接选择整个当前网段；选中“忽略 IP [0]”复选框，可以屏蔽所有以 0 结尾的 IP 地址；选中“忽略 IP [255]”复选框，可以屏蔽所有以 255 结尾的 IP 地址。另外，也可以选中“从文件中读取”复选框，然后单击其右侧的按钮，在弹出的对话框中选择域名列表文件，从中获取 IP 地址列表。

STEP 04 设置扫描端口

单击窗口右上角的“端口列表”按钮，在弹出的“编辑端口列表”对话框中可以设置扫描端口。在“选择端口”选项区的列表框中双击要扫描的端口，当端口的左侧出现一个✓号时，表示已选中此端口，如下图所示。



基础知识

与嗅探工具

系统漏洞攻防

安全策略

系统与安全

远程控制

木马

聊天软件

网页篡改

代码攻击

件攻击

电子邮

攻击防

使用电脑

黑客攻防



STEP 05 修改扫描端口信息

在“修改/新增/删除端口信息”选项区中可以对端口信息进行编辑，如修改 21 端口的描述信息为“文件传输控制”，只需在“描述”文本框中输入相应信息即可，如下图所示。编辑好端口修改信息后，单击“应用”按钮即可应用当前设置。



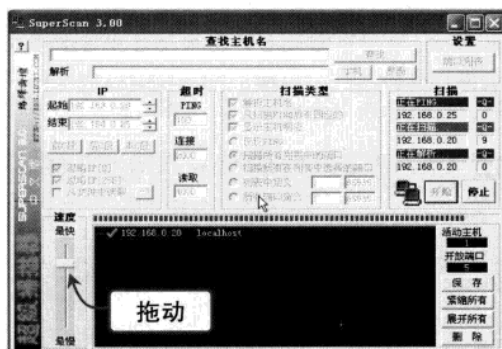
STEP 06 添加木马端口扫描列表

在“端口列表文件”选项区中可以设置木马端口扫描列表，单击“读取”按钮，在弹出的对话框中选择相应的端口列表文件，然后单击“打开”按钮返回，这里直接在下拉列表框中选择 scanner.lst 选项，如下图所示。



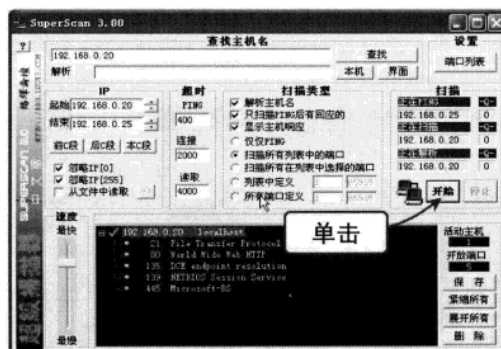
STEP 07 调整扫描速度

单击“确定”按钮返回扫描器主工作窗口，在“速度”选项区中上下拖动滑块，可以调整扫描速度，如下图所示。



STEP 08 查看扫描结果信息

单击“开始”按钮，系统开始对所设置的端口进行扫描，当扫描结束后即可看到扫描到的主机及其端口信息，如下图所示。



提示



扫描完成后，单击右下角的“展开所有”按钮，扫描到的详细信息就会显示出来，包括对方开放的端口以及相应的服务，单击“删除”按钮，程序就会自动过滤掉那些没有扫描到的主机。

为了更好地进行扫描工作，这里将一些系统常用的服务端口列了出来，读者可以进行参考。

- ❖ 21 端口：文件传输协议（FTP）。
- ❖ 22 端口：SSH（安全 shell），通常只在 UNIX/Linux 下开放。
- ❖ 23 端口：Telnet 服务。
- ❖ 25 端口：SMTP 邮件服务。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 02 常用扫描与嗅探工具

- ❖ 53 端口：域名服务。
- ❖ 80 端口：Web 服务，通常网站都会开放 80 端口。
- ❖ 111 端口：SUN Remote Procedure Call，通常只会在 UNIX/Linux 下开放。
- ❖ 135 端口：DCE endpoint resolution，Windows 系统默认开放。
- ❖ 139 端口：NETBIOS 服务，Windows 系统默认开放。
- ❖ 389 端口：LDAP（Lightweight Directory Access Protocol），轻量级目录访问协议，通常只在 UNIX/Linux 开放。
- ❖ 443 端口：http Mcom，通常只在 UNIX/Linux 下开放。
- ❖ 445 端口：Microsoft-DS，Windows 系统默认开放。
- ❖ 554 端口：Real Time Stream Control Protocol，Real Time 流控制协议。
- ❖ 1433 端口：Microsoft-SQL 服务。
- ❖ 3306 端口：MySQL 服务。
- ❖ 3389 端口：Windows 的终极服务。

2.4 常见多功能扫描器

除了上面讲述的两种端口扫描器以外，还有很多具备诸多不同功能的扫描器，黑客们比较常用的多功能扫描器有流光扫描器、SSS 扫描器、X-scan 扫描器等，下面将分别进行介绍。

2.4.1 流光扫描器

流光扫描器是一款非常出名的中文多功能专业扫描器，其功能强大、扫描速度快、可靠性强，为广大电脑黑客迷们所钟爱。

流光扫描器可以探测 POP3、FTP、HTTP、PROXY、FROM、SQL、SMTP 和 IPC 等各种漏洞，并针对各种漏洞设计不同的破解方案。其主要功能如下：

- ❖ 用于检测 POP3/FTP 主机中的用户密码安全漏洞。
- ❖ 多线程检测，用于消除系统中的密码漏洞。
- ❖ 高效的用戶流模式。
- ❖ 高效的服务器流模式，可以同时多台 POP3/FTP 主机进行检测。
- ❖ 最多 500 个线程探测。
- ❖ 线程超时设置，阻塞线程具有自杀功能，不会影响其他线程。
- ❖ 支持 10 个字典同时检测。
- ❖ 检测设置可以作为项目保存，以便下次继续调用。

Work1 探测开放端口

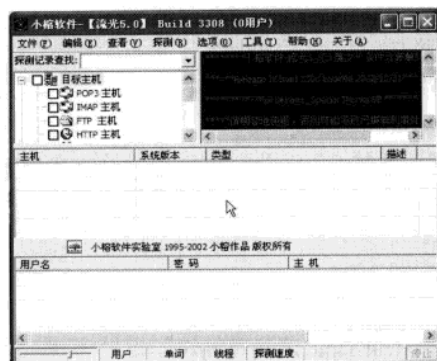
利用流光扫描器可以轻松探测目标主机的开放端口，下面以探测 POP3 主机的开放端口为例进行介绍。

STEP 01 启动流光扫描器

单击桌面上的流光扫描器程序图标，启动流光扫描器，如下图所示。

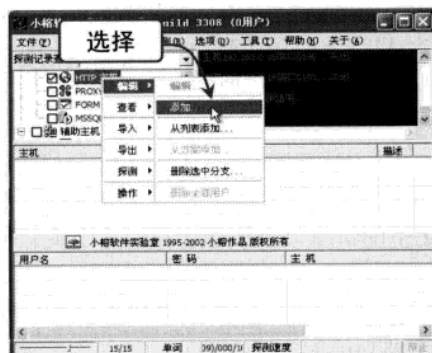
STEP 02 打开“系统设置”对话框

单击“选项”|“系统设置”命令，打开“系统设置”对话框，对优先级、线程数、单词数/线程及扫描端口进行设置，如下图所示。



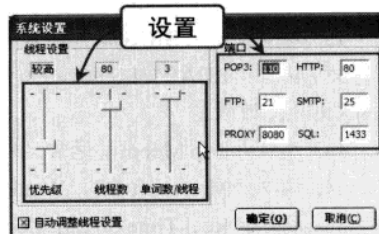
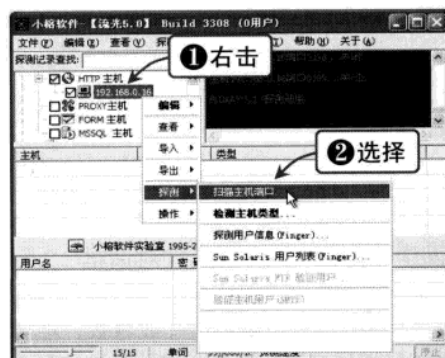
STTP 03 选择“编辑”|“添加”选项

在扫描器主窗口中选中“HTTP 主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”|“添加”选项，如下图所示。



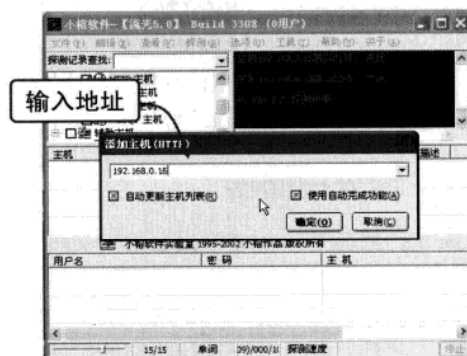
STTP 05 选择“扫描主机端口”选项

此时在主窗口中将显示出刚刚添加的 HTTP 主机，右击此主机，在弹出的快捷菜单中依次选择“探测”|“扫描主机端口”选项，如下图所示。



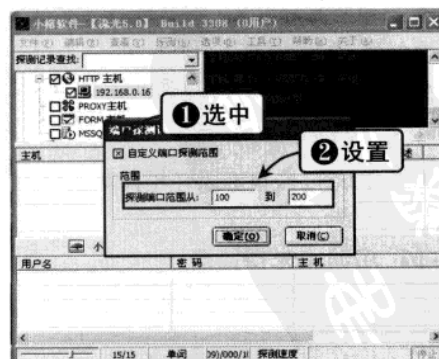
STTP 04 输入要扫描主机的 IP 地址

打开“添加主机 (HTTP)”对话框，在该对话框的下拉列表框中输入要扫描主机的 IP 地址（这里以 192.168.0.16 为例），如下图所示。



STTP 06 设置探测端口范围

打开“端口探测设置”对话框，在该对话框中选中“自定义端口探测范围”复选框，然后在“范围”选项区中设置要探测端口的范围，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 02 常用扫描与嗅探工具

STEP 07 开始探测开放端口

设置完成后，单击“确定”按钮，开始探测目标主机的开放端口，如下图所示。



STEP 08 显示探测结果

扫描完毕后，将会自动弹出“探测结果”对话框，如果目标主机存在开放端口，就会在该对话框中显示出来，如下图所示。



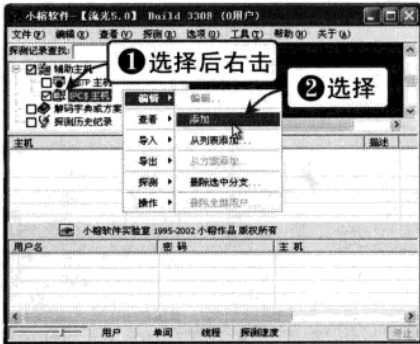
Work2 探测目标主机的 IPC\$ 用户列表

IPC\$（Internet Process Connection）是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用 IPC\$ 可以与目标主机建立一个空的连接，利用这个空的连接，连接者可以获得目标主机上的用户列表，通过猜测密码或者穷举密码，从而获得管理员权限。利用流光扫描器探测目标主机的 IPC\$ 用户列表的具体操作方法如下：

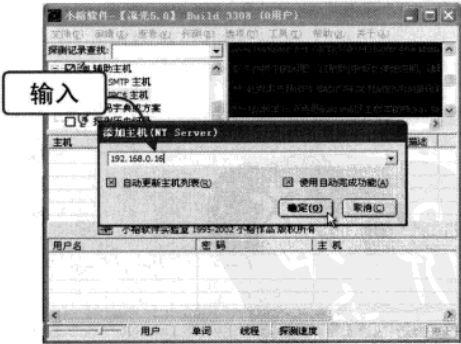
STEP 01 选择“编辑”|“添加”选项

在流光扫描器主窗口中选中“IPC\$ 主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”|“添加”选项，如下图所示。



STEP 02 添加 IPC\$ 扫描目标主机

打开“添加主机（NT Server）”对话框，在其下拉列表框中输入要扫描主机的 IP 地址（这里以 192.168.0.16 为例），如下图所示。



STEP 03 选择“探测 IPC\$ 用户列表”选项

选中刚刚添加的 IPC\$ 主机，然后右击，在弹出的快捷菜单中选择“探测”|“探测 IPC\$ 用户列表”选项，如下图所示。

STEP 04 设置自动探测选项

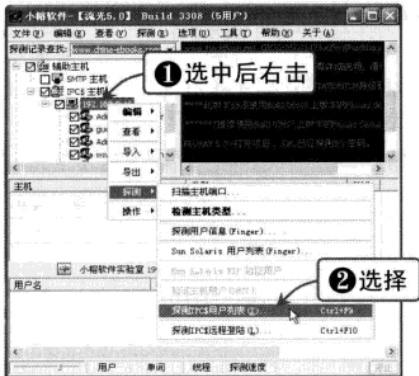
打开“IPC 自动探测”对话框，在该对话框中单击“选项”按钮，在打开的“用户列表选项”对话框中进行设置，如下图所示。

黑客
基础知识
常用扫描与嗅探工具
Windows 系统
漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电
脑安全软
件
黑客攻
防技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

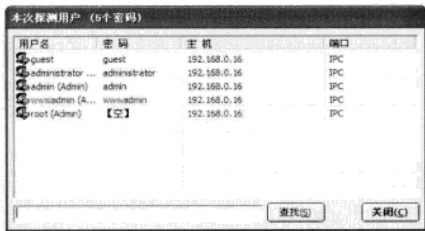


黑客攻防从新手到高手



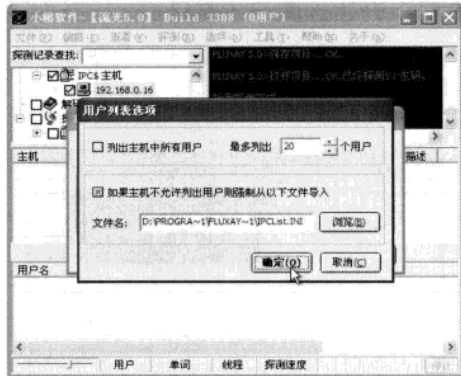
STEP 05 查看探测结果

单击“确定”按钮，程序开始自动探测目标主机。扫描完成后会弹出一个探测结果对话框，其中列出了探测到的用户名和密码信息，如下图所示。



STEP 07 打开“命令提示符”窗口

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入命令 cmd，按【Enter】键，即可打开“命令提示符”窗口，如下图所示。



STEP 06 查看检测报告

单击“关闭”按钮，系统将弹出一个提示信息框，提醒用户是否生成检测报告，单击“是”按钮，即可查看检测报告，如下图所示。



STEP 08 与目标主机建立 IPC 连接

根据刚刚探测到的 IPCS 用户名和密码，在“命令提示符”窗口中输入相应的命令，即可与目标主机建立 IPC 连接，如下图所示。



Work3 扫描指定地址范围内的目标主机

使用流光扫描器的高级扫描向导，可以快速地对指定地址范围内的目标主机进行扫描，

Chapter 02 常用扫描与嗅探工具

其具体操作步骤如下：

STEP 01 单击“高级扫描向导”命令

在流光扫描器主窗口中单击“文件”|“高级扫描向导”命令，如下图所示。



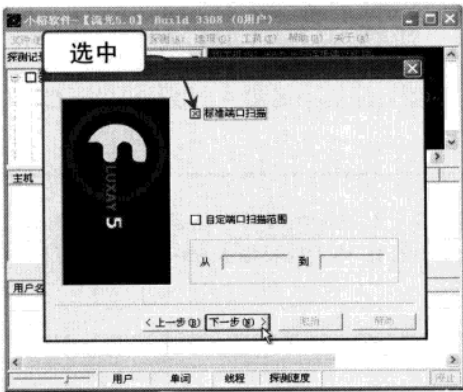
STEP 02 添加指定地址范围

打开“设置”对话框，在“起始地址”和“结束地址”文本框中分别输入指定地址范围的开始和结束 IP 地址，并选中“获取主机名”和“PING 检查”复选框，如下图所示。



STEP 03 设置要扫描的端口范围

单击“下一步”按钮，弹出 POSTS 对话框，在该对话框中对要扫描的端口范围进行设置，这里选中“标准端口扫描”复选框，如下图所示。



STEP 04 设置 POP3 检测项目

单击“下一步”按钮，打开 POP3 对话框，在该对话框中可以对 POP3 检测项目进行设置，这里选中“获取 POP3 版本信息”和“尝试猜解用户”复选框，如下图所示。



STEP 05 设置 IPC 检测项目

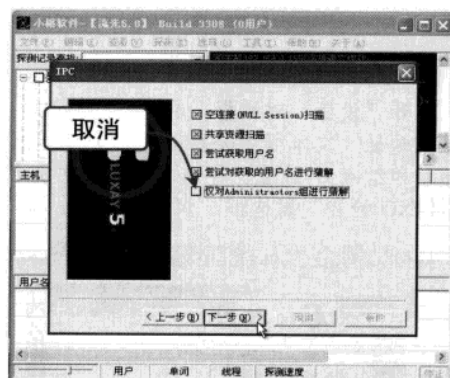
依次单击“下一步”按钮，打开 IPC 对话框，在该对话框中可以对 IPC 检测项目进行设置，这里取消选择“仅对 Administrators 组进行猜解”复选框，如下图所示。

STEP 06 设置字典和扫描报告路径

依次单击“下一步”按钮，直至系统弹出“选项”对话框，在该对话框中设置“猜解用户名字典”、“猜解密码字典”和“保存扫描报告”的路径，如下图所示。

黑客
基础知识
常用扫描
与嗅探工具
系统漏洞攻防
安全策略
设置系统
系统与文
件加密
远程控制
木马
聊天软
网页恶
代码攻
件攻
毒攻
使用电
安全软
黑客攻
实用技

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



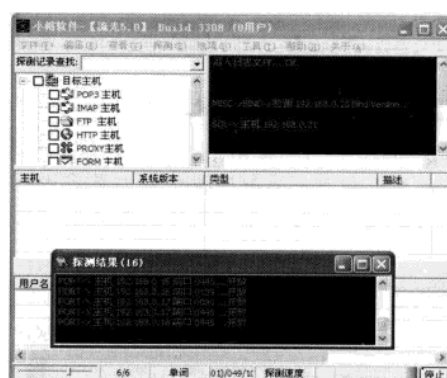
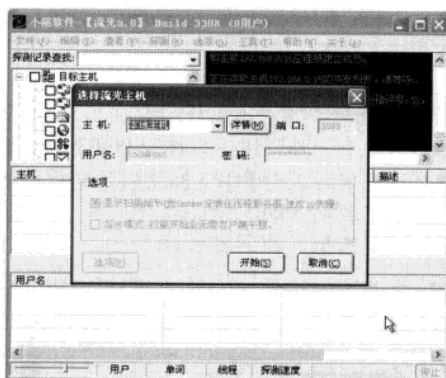
STEP 07 “选择流光主机”对话框

单击“完成”按钮，弹出“选择流光主机”对话框，如下图所示。



STEP 08 开始探测目标主机

单击“开始”按钮，程序开始扫描指定的地址范围，这可能需要较长时间，在扫描过程中还会打开探测结果对话框提示用户，如下图所示。



提示

扫描完毕后，系统会弹出“注意”提示信息框提醒用户是否要查看扫描报告，单击“是”按钮，此时会打开一个HTML格式的扫描报告，其中列出了扫描到的主机的详细信息。

2.4.2 SSS 扫描器

SSS 扫描器是一款来自俄罗斯的老牌安全扫描软件，具有非常专业的安全漏洞扫描功能，能够扫描出计算机中存在的各种漏洞，是网络黑客必备软件之一。

SSS 扫描器能够对很大范围内的系统漏洞进行安全、可靠、高效的检测，如果发现系统存在被攻击的漏洞，就会给用户相应的解决方法。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

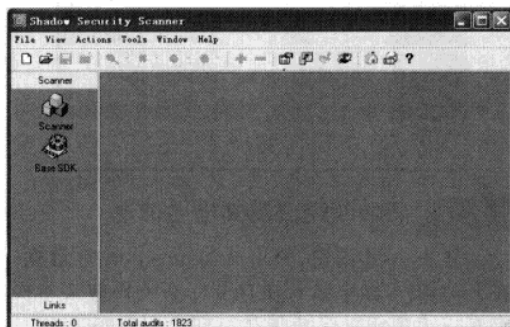
Chapter 02 常用扫描与嗅探工具

Work1 设置功能选项参数

在使用 SSS 扫描器之前，需要先对其各功能选项进行设置，具体操作步骤如下：

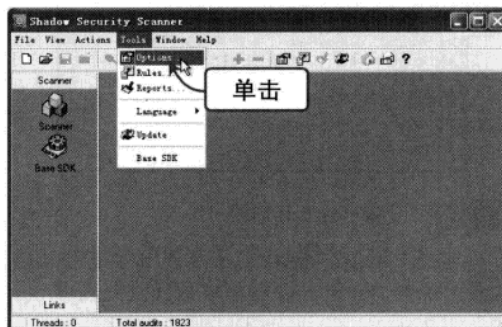
STEP 01 打开 SSS 扫描器主窗口

双击桌面上的 Shadow Security Scanner 图标, 即可打开 SSS 扫描器主窗口, 如下图所示。



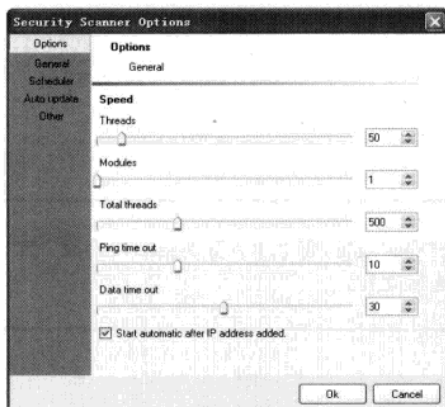
STEP 02 打开选项设置窗口

单击 Tools | Options 命令，如下图所示，打开 Security Scanner Options 对话框。



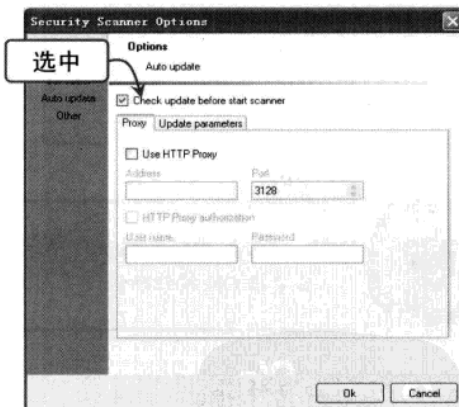
STEP 03 设置扫描速度

在 General 选项界面中设置扫描速度,其中 Threads 表示线程数,设置的线程数越大,扫描的速度也就越快; Modules 表示扫描的模块; Total threads 表示总线程数,如下图所示。



STEP 04 设置软件自动升级参数

选中 Start automatic after IP address added 复选框, 然后选择 Auto update 选项界面中设置软件自动升级参数, 其主要选项如下图所示。SSS 扫描器更新频率很快, 因此这里建议选中 Check update before start scanner 复选框。



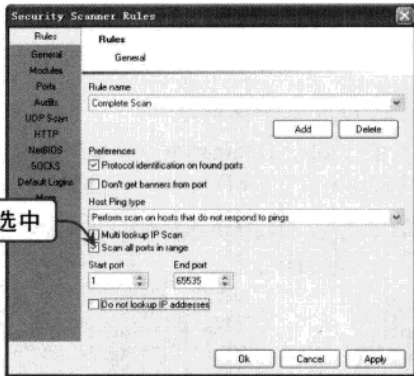
STEP 05 设置扫描端口

单击 OK 按钮返回主窗口, 单击 Tools | Rules 命令, 打开 Security Scanner Rules 对话框, 选择 General 选项界面, 在这里可以对扫描端口进行设置, 在 Rules name 下拉列表框中选择 Complete Scan 选项, 并在下方选中 Scan all ports in range 复选框, 如下图所示。

STEP 06 设置扫描模块

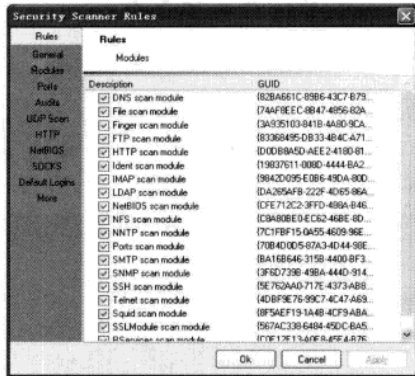
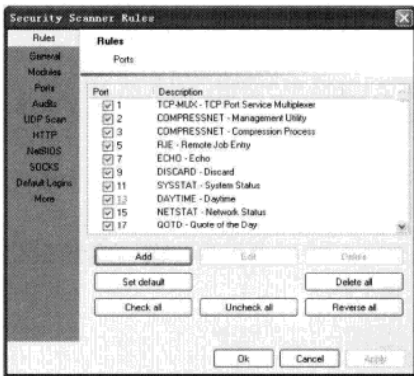
选择 **Modules** 选项界面，在右侧窗格中可以选中需要的扫描模块。选中的选项越多，表示要扫描的模块越多，而扫描需要的时间也相应变长。当对某台主机进行扫描时，用户可以将这些模块都选中，这样扫描出的效果会更好，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



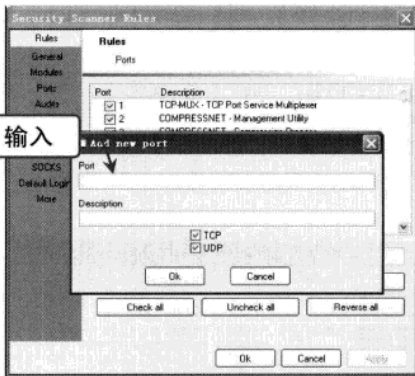
STEP 07 设置 Ports 选项

选择 Ports 选项界面，在右侧窗格中可以添加或删除端口，还可以对端口的描述进行修改，如下图所示。

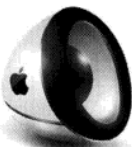


STEP 08 添加新端口及其描述信息

单击 Add 按钮，弹出 Add new port 对话框，在 Port 文本框中输入端口号，在下面的文本框中可以添加端口描述信息，如下图所示。



提示



单击 OK 按钮返回，在 Security Scanner Rules 窗口中设置其他相应参数，然后单击 OK 按钮确认设置，完成功能选项设置。

Work2 定制扫描任务

在 SSS 扫描器中，还可以提前制定扫描任务，让软件按照指定的时间对指定目标进行扫描，具体操作步骤如下：

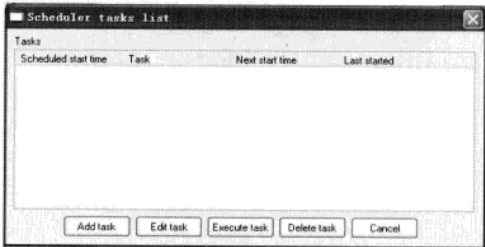
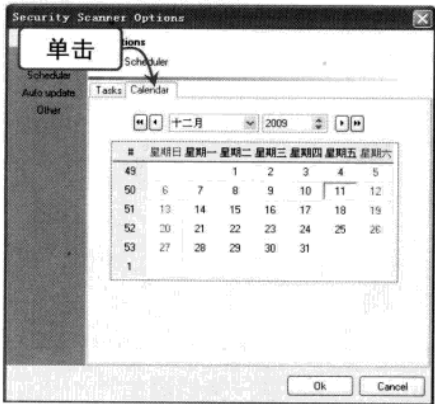
STEP 01 打开 Scheduler 选项界面

在 SSS 扫描器主窗口中单击 Tools | Options 命令，打开 Security Scanner Options 窗口，打开 Scheduler 选项界面，并单击 Calendar 选项卡，如下图所示。

STEP 02 调整日期

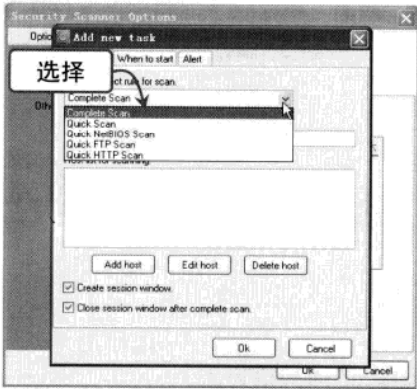
此时可以看到一个日期面板，在此可以调整任务的年份、月份及日期，双击选定的日期，弹出 Scheduler tasks list 对话框，如下图所示。

Chapter 02 常用扫描与嗅探工具



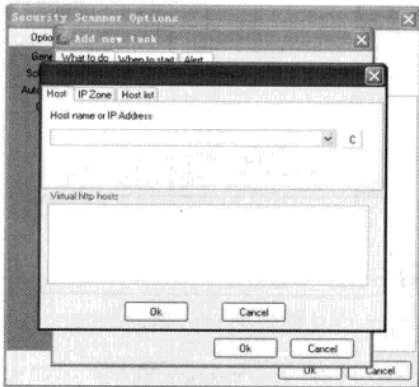
STEP 03 选择扫描方式

单击 Add task 按钮，弹出 Add new task 对话框，选择 What to do 选项卡，在 Please, select rule for scan 下拉列表框中选择 Complete Scan 选项，如下图所示。



STEP 04 设置扫描范围

单击 Add host 按钮，在弹出的对话框中可以选择 Host 选项卡设置对一个单一 IP 地址进行扫描，也可以选择 IP Zone 选项卡指定扫描范围，还可以选择 Host list 选项卡选择扫描 IP 列表文件。



提示

Complete Scan 表示完整扫描；Quick Scan 表示快速扫描；Quick NetBIOS Scan 表示进行 NetBIOS 扫描；Quick FTP Scan 表示进行 FTP 扫描；Quick HTTP Scan 表示进行 HTTP 扫描。

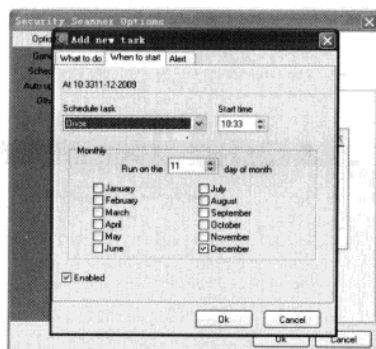
STEP 05 设置扫描时间

单击 OK 按钮返回 Add new task 对话框，选择 When to start 选项卡，在这里可以对扫描任务的开始时间进行设置，如下图所示。

STEP 06 添加扫描任务相关信息

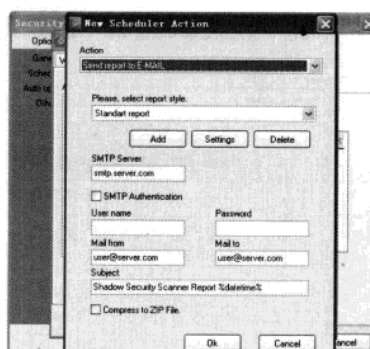
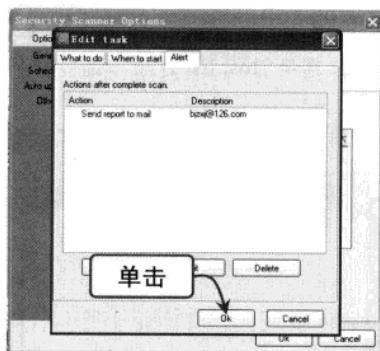
单击 OK 按钮返回 Add new task 对话框，选择 Alert 选项卡，单击 Add 按钮，打开 New Scheduler Action 对话框，添加扫描任务的相关信息，如下图所示。

基础知
与嗅探工
统漏洞攻
安全策
件加密
制攻防
攻防
件攻防
代码防
件攻防
毒攻防
安全软
实用技



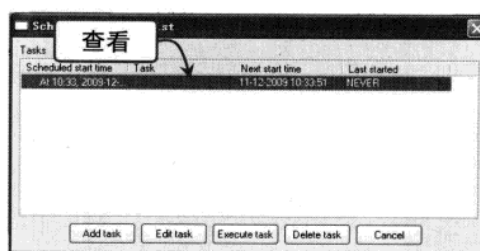
STEP 07 返回 Add new task 对话框

在该对话框中添加好扫描结果发送到的邮箱地址，然后单击 OK 按钮返回 Edit task 对话框，如下图所示。



STEP 08 完成扫描任务的添加

单击 OK 按钮返回 Scheduler tasks list 对话框，在下面的列表中可以查看刚刚添加的扫描任务，如下图所示。

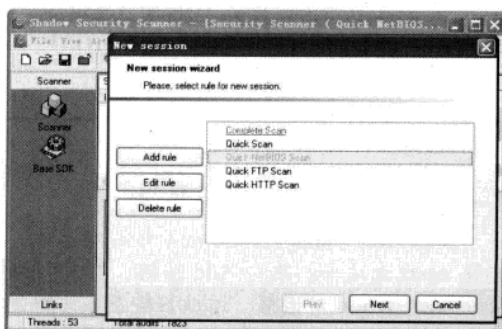


Work3 扫描系统漏洞

利用 SSS 扫描器扫描系统漏洞的具体操作步骤如下：

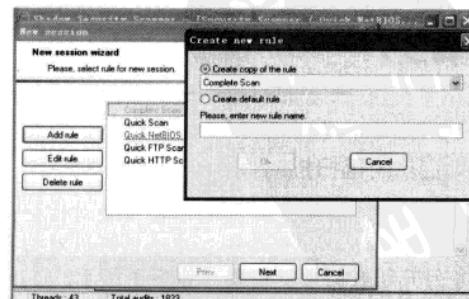
STEP 01 打开 New session 窗口

在 SSS 扫描器主窗口中单击 Scanner 按钮，打开 New session 对话框，如下图所示。



STEP 02 选择扫描方式

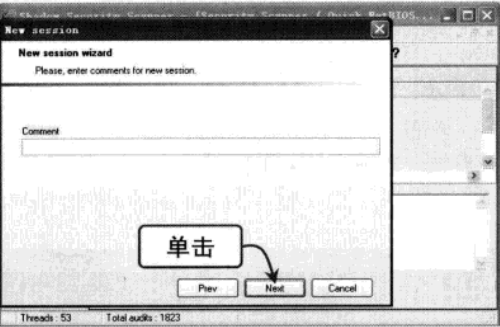
在右侧列表中选择系统预设的扫描方式，也可以单击 Add rule 按钮，在弹出的对话框中添加新的扫描方式，如下图所示。



Chapter 02 常用扫描与嗅探工具

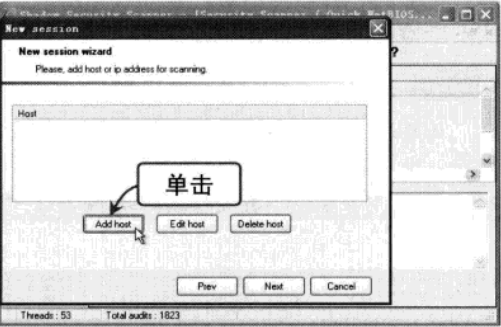
STEP 03 添加注释

单击 Next 按钮，在弹出的对话框中添加注释信息，如下图所示。



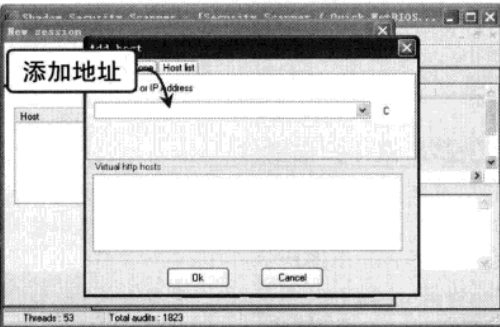
STEP 04 添加主机

单击 Next 按钮，在弹出的对话框中单击 Add host 按钮添加扫描主机，如下图所示。



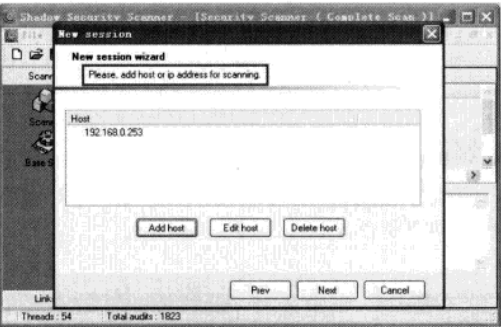
STEP 05 设置扫描 IP 范围

在弹出的 Add host 对话框中添加扫描 IP 地址或某地址段，如下图所示。



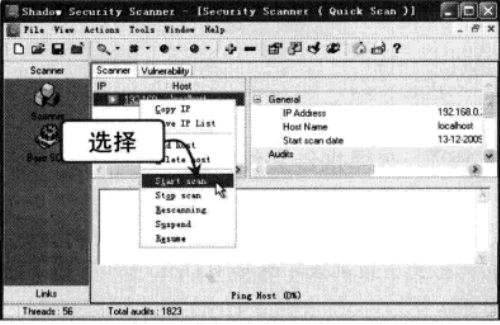
STEP 06 返回 New session 窗口

单击 OK 按钮返回 New session 窗口，即可看到刚刚添加的扫描地址，如下图所示。



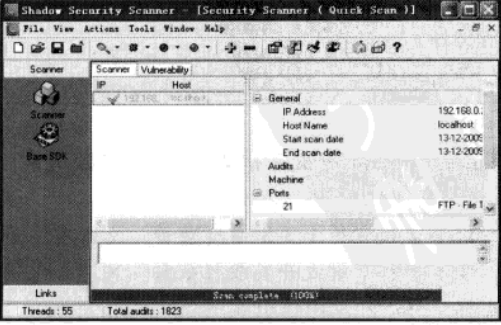
STEP 07 选择 Start scan 选项

单击 Next 按钮返回主窗口，右击刚刚添加的扫描任务，然后在弹出的快捷菜单中选择 Start scan 选项，如下图所示。



STEP 08 完成扫描任务的添加

系统开始对目标主机进行扫描，当检测完毕后，右侧窗格中会显示出该计算机的系统信息和开放端口情况，如下图所示。



黑客
常用扫描
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
件攻防
网页恶意
代码攻防
电子邮件
C 盘病毒
使用电脑
黑客攻防
实用技巧

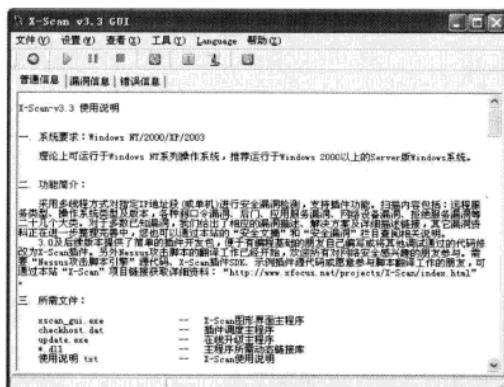


2.4.3 X-Scan 扫描器

X-Scan 扫描器是一款功能强大的安全漏洞扫描器，它能够准确地检测出用户计算机中的各种漏洞和弱口令信息，是黑客常用的多功能扫描工具之一。使用 X-Scan 扫描器进行系统安全检测的具体操作步骤如下：

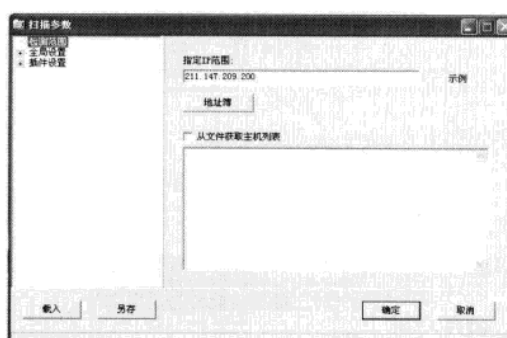
STEP 01 打开 X-Scan 扫描器主窗口

从网站上下载 X-Scan 扫描器，然后运行该软件，打开其主窗口，如下图所示。



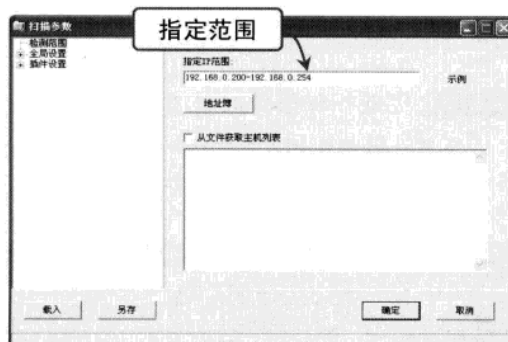
STEP 02 打开“扫描参数”对话框

单击“设置”|“扫描参数”命令，打开“扫描参数”对话框，如下图所示。



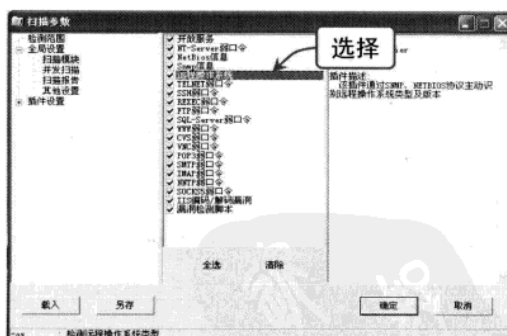
STEP 03 指定扫描 IP 地址段

在“指定 IP 范围”文本框中指定 IP 地址段，如下图所示。



STEP 04 选择扫描插件

在左侧窗格中展开“全局设置”选项，然后选择“扫描模块”选项，在中间窗格中选择扫描插件，如下图所示。



STEP 05 设置并发主机数量和线程数量

在左侧窗格中选择“并发扫描”选项，在右侧窗格的“最大并发主机数量”文本框中输入数量，在“最大并发线程数量”文本框中输入线程数，如下图所示。

STEP 06 选择报告文件类型

在左侧窗格中选择“扫描报告”选项，在右侧窗格中单击“报告文件类型”下拉列表框，在弹出的下拉列表中选择 HTML 选项，如下图所示。



2.5 常用网络嗅探工具

网络嗅探是指利用计算机的网络接口截获目的地为其他计算机的数据报文的一种手段。网络嗅探的基础是数据捕获，网络嗅探系统是并接在网络中来实现对于数据的捕获的，这种方式和入侵检测系统相同，因此被称为网络嗅探。

网络嗅探需要用到网络嗅探器，其最早是为网络管理人员配备的工具。有了嗅探器网络管理员可以随时掌握网络的实际情况，查找网络漏洞和检测网络性能，当网络性能急剧下降的时候，可以通过嗅探器分析网络流量，找出网络阻塞的来源。

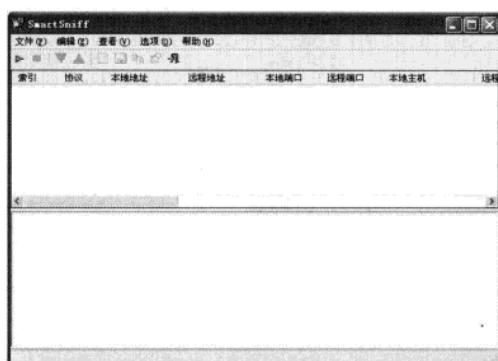
2.5.1 嗅探利器 SmartSniff

SmartSniff 可以让用户捕获自己的网络适配器的 TCP/IP 数据包，并且可以按顺序查看客户端与服务器之间会话的数据。用户可以使用 ASCII 模式（用于基于文本的协议，如 HTTP、SMTP、POP3 与 FTP）或十六进制模式来查看 TCP/IP 会话（用于基于非文本的协议，如 DNS）。

利用 SmartSniff 捕获 TCP/IP 数据包的具体操作步骤如下：

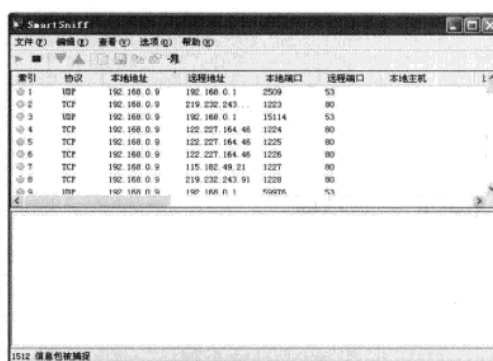
STEP 01 打开 SmartSniff 程序主窗口

单击桌面上的 SmartSniff 程序图标，打开 SmartSniff 程序主窗口，如下图所示。



STEP 02 开始捕获数据

单击“开始捕捉”按钮或按【F5】键，开始捕获当前主机与网络服务器之间传输的数据包，如下图所示。



STEP 03 查看 TCP 协议类型的数据包

单击“停止捕获”按钮或按【F6】键，停止捕获数据，在列表中选择任意一个 TCP 协议类型的数据包，即可查看其数据信息，如下图所示。

STEP 04 查看 UDP 协议类型的数据包

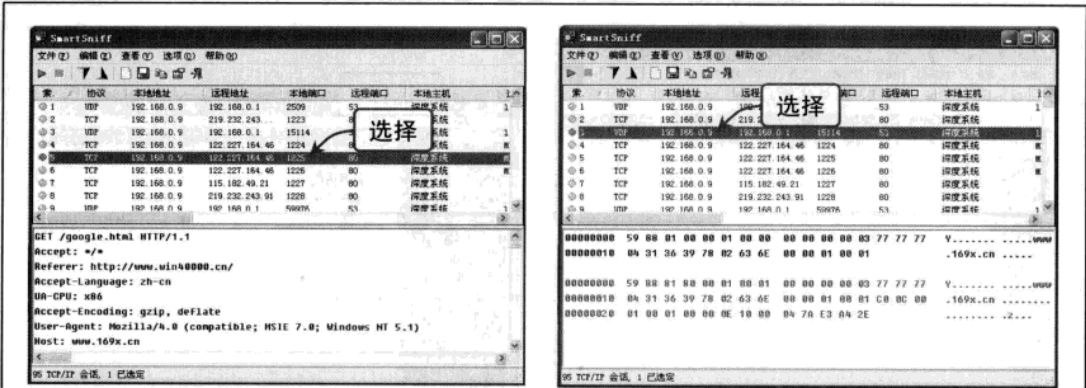
在列表中选择任意一个 UDP 协议类型的数据包，即可查看其数据信息，如下图所示。



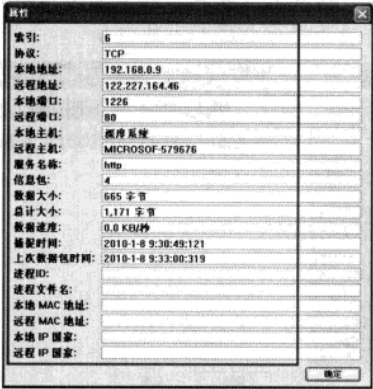
提示

从列表中可以看到，所捕获的数据包多为 TCP 和 UDP 两种协议类型，而这两种数据信息的表示方式也略有不同。

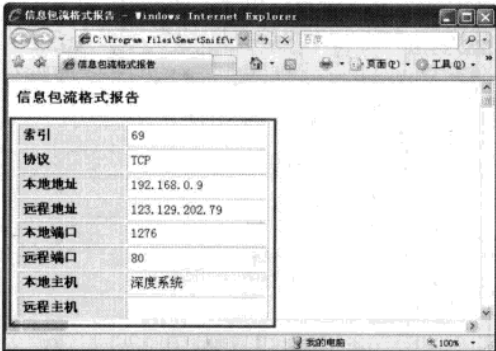
Chapter 02 常用扫描与嗅探工具



STEP 05 查看数据包属性信息
在列表中选中任意一个数据包，单击“文件”|“属性”命令，在弹出的“属性”对话框中可以查看其属性信息，如下图所示。



STEP 06 用“ping+空格+网站地址”格式
在列表中选中任意一个数据包，单击“查看”|“HTML 报告-TCP/IP 流格式”命令，可以网页形式查看信息包流格式报告，如下图所示。



2.5.2 Iris 网络嗅探器

Iris 是一款非常优秀的网络通信分析工具（全称 Iris Network Traffic Analyzer），由著名的网络安全公司 eEye Digital Security 开发。它可以帮助系统管理员轻易地捕获和查看进出网络的数据包，进行分析和解码并生成多种形式的统计图表，它可以探测本机端口和网络设备的使用情况，有效地管理网络通信。相对于其他网络嗅探器，Iris 更加易用和人性化，以多元化的模块满足不同层次用户的需求，是网络管理人员和分析人员的必备工具。

Work1 Iris 网络嗅探器的设置

在使用 Iris 网络嗅探器之前，需要先对其选项进行相应设置，具体操作方法如下：

STEP 01 打开 Iris 网络嗅探器工作窗口

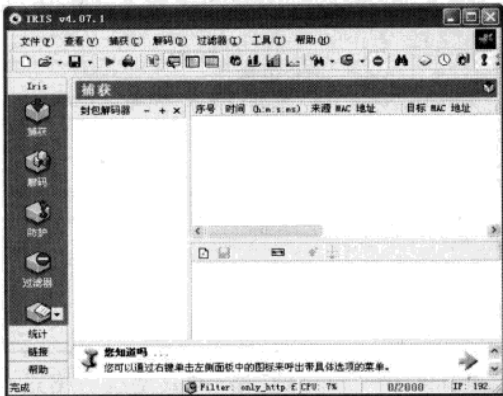
运行 Iris 网络嗅探器，打开其工作窗口，如下图所示。

STEP 02 设置捕获选项

单击“工具”|“设置”命令，打开“设置”对话框，如下图所示。在左侧窗格中选择“捕获”选项，在右侧窗格中可以对捕获动作、载入的过滤器等进行设置。

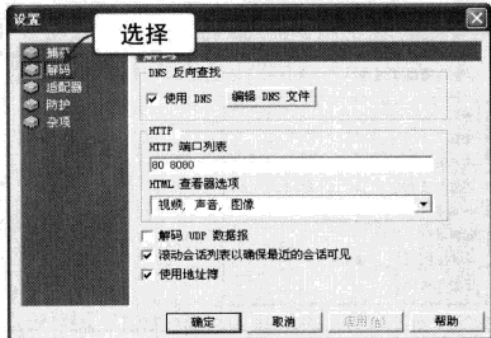
黑客
基础知识
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程程
控
木马
聊天软
件攻防
网页恶
意
代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电
脑
安全软
件
黑客攻
防技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



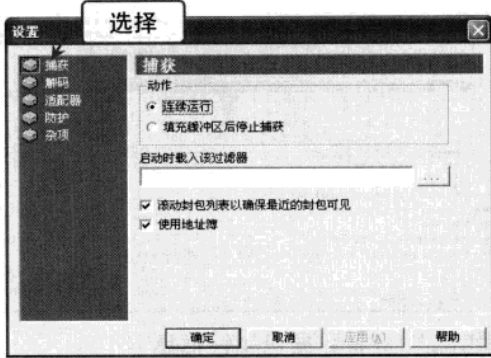
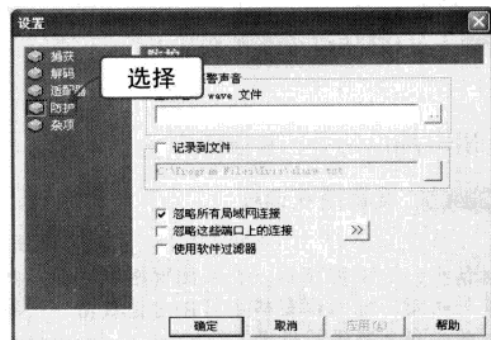
STEP 03 设置解码选项

在左侧窗格中选择“解码”选项，在右侧窗格中可以设置 DNS 反向查找、HTTP 端口列表和 HTML 查看器选项等，如下图所示。



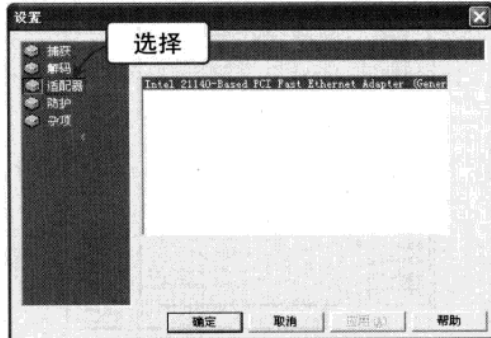
STEP 05 设置防护选项

在左侧窗格中选择“防护”选项，在右侧窗格中可以设置在捕获数据时的防护措施，如下图所示。



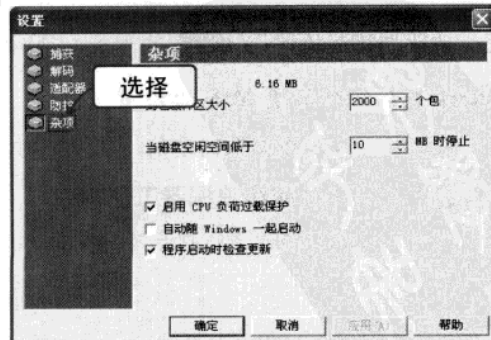
STEP 04 设置适配器选项

如果用户计算机有多个网卡，在左侧窗格中选择“适配器”选项，在右侧窗格中可以设置当前捕获哪一个网卡上的数据，如下图所示。



STEP 06 设置杂项选项

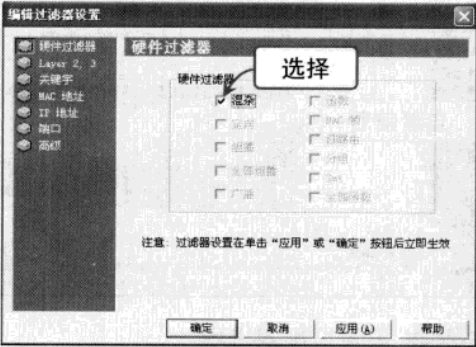
在左侧窗格中选择“杂项”选项，在右侧窗格中可以对内存和磁盘空间进行设置，还可以选择是否随 Windows 一起启动和检查更新，如下图所示。



Chapter 02 常用扫描与嗅探工具

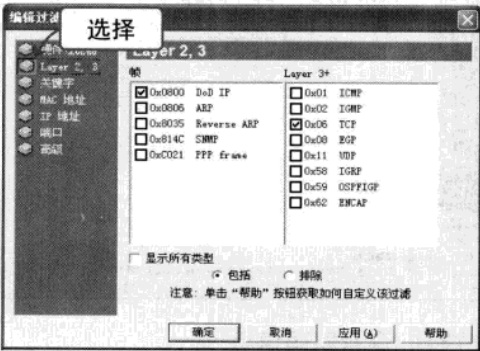
STEP 07 设置硬件过滤器选项

单击“过滤器”|“编辑过滤器”命令，打开“编辑过滤器设置”对话框，在左侧窗格中选择“硬件过滤器”选项，在右侧窗格中可以设置硬件过滤器，系统默认选中“混杂”复选框，如下图所示。



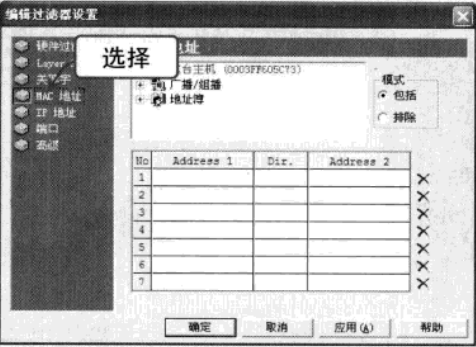
STEP 08 设置“Layer2, 3”选项

在左侧窗格中选择“Layer2, 3”选项，在右侧窗格中可以设置如何对网络体系结构中的第2和第3层数据进行过滤，如下图所示。其中，选中“包括”单选按钮，表示必须都符合所选条件才进行捕获；选中“排除”单选按钮，表示符合所选条件之一即可进行捕获。



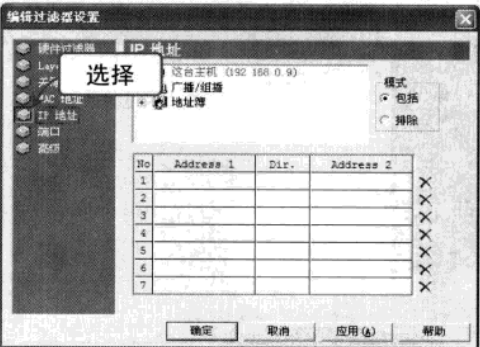
STEP 09 设置 MAC 地址列表

在左侧窗格中选择“MAC 地址”选项，在右侧窗格中可以设置 MAC 地址列表，如下图所示。



STEP 10 设置 IP 地址列表

在左侧窗格中选择“IP 地址”选项，在右侧窗格中可以设置 IP 地址列表，如下图所示。



提示

在“编辑过滤器设置”对话框的左侧窗格中分别选择“端口”和“高级”选项，用户还可以对过滤端口和封包大小等进行设置。

Work2 使用 Iris 捕获数据

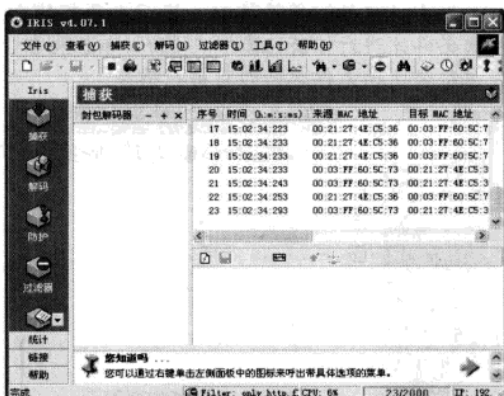
设置好相应的选项后，用户就可以使用 Iris 网络嗅探器捕获数据了。下面将通过一个简单的实例简单介绍使用 Iris 网络嗅探器捕获数据的方法，具体操作步骤如下：

基础知识
常用扫描
与嗅探工具
系统与安全
漏洞攻防
安全策略
系统与安全
件加密
远程控制
攻击
木马
聊天软件
网页恶意
代码攻防
件攻防
电子邮件
C 盘病毒
使用电脑
黑客攻防
实用技巧



STEP 01 开始捕获数据

在 Iris 网络嗅探器工作窗口中单击“捕获”|“开始”命令，嗅探器开始捕获通过网络适配器传输的数据，如下图所示。



STEP 02 查看封包相关信息

在“捕获”窗口的栏目列表中可以看到捕获的封包列表，选择任意一个封包，可以查看其相关信息，如下图所示。



STEP 03 查看解码信息

单击“查看”|“显示解码视图”命令，可以打开解码视图，用户在该环境下可以查看所选封包的解码信息，如下图所示。



STEP 04 设置适配器选项

在解码视图中选择 HTTP 数据包，对其显示解码后还可以显示所查看网页的有关信息，如下图所示。



2.5.3 网络数据包嗅探专家

网络数据包嗅探专家是一款监视网络数据运行的嗅探器，它能够完整地捕捉到所处局域网中所有计算机的上行、下行数据包，用户可以将捕捉到的数据包保存下来，以进行监视网络流量、分析数据包、查看网络资源利用、执行网络安全操作规则、鉴定分析网络数据以及诊断并修复网络问题等操作。

另外，该软件不仅能找出隐藏在网页中的媒体文件的网络地址，还能让影视软件上的流媒体地址无处遁形，并且该软件还能找出很多其他格式的资源文件的网络地址，可用于本地网络安全、网页、电影地址嗅探、局域网管理、网络程序设计等辅助工作。

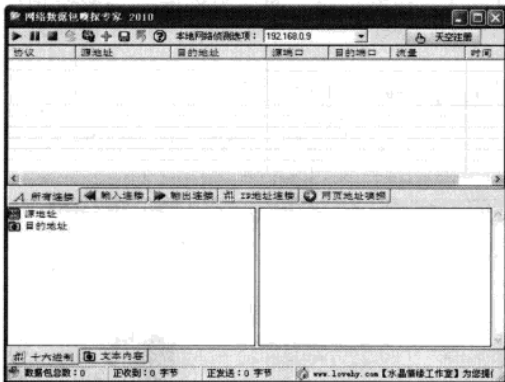
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 02 常用扫描与嗅探工具

使用网络数据包嗅探专家的具体操作方法如下：

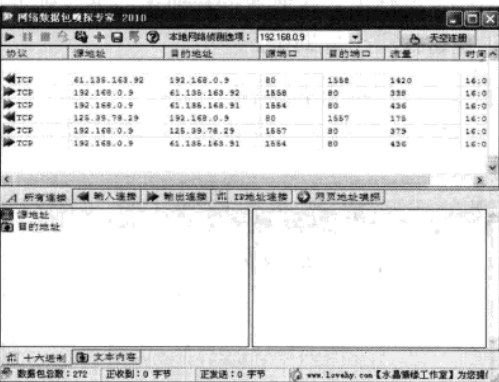
STEP 01 打开网络数据包嗅探专家

打开网络数据包嗅探专家程序，其工作界面如下图所示。



STEP 02 开始捕获数据

单击“开始嗅探”按钮，开始捕获当前网络数据，如下图所示。



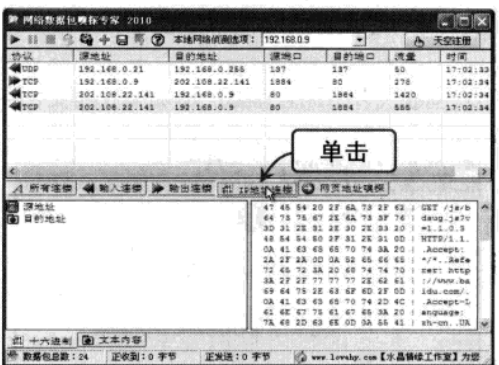
STEP 03 单击“停止嗅探”按钮

单击“停止嗅探”按钮，停止捕获数据包，当前的所有网络连接数据将在下方显示出来，如下图所示。



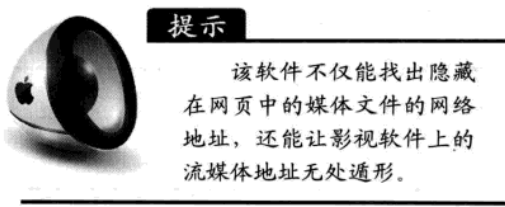
STEP 04 单击“IP 地址连接”按钮

单击“IP 地址连接”按钮，将在上方窗格中显示前一段时间内输入与输出数据的源地址与目标地址，如下图所示。



STEP 05 单击“网页地址嗅探”按钮

单击“网页地址嗅探”按钮，即可查看当前所连接网页的详细地址和文件类型，如右图所示。



提示

该软件不仅能找出隐藏在网页中的媒体文件的网络地址，还能让影视软件上的流媒体地址无处遁形。

黑客
基础入门
与黑客工具
Windows 系统
系统设置
安全策略
系统安全
系统加密
远程控制
木马
聊天软件
网页攻击
代码攻击
电子攻击
C 盘病毒
使用电脑
黑客技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

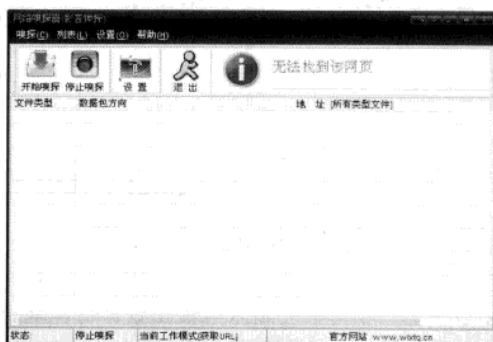


2.5.4 影音神探

随着网络的普及，我们现在已经习惯在互联网上下载所需的文件，而电影和音乐更是我们经常下载的东西。但互联网上很多影音文件下载时须付费，无法直接通过网页免费下载。遇到这种情况，就要通过其他途径来达到下载目的，所幸的是，网络嗅探器——影音神探正是这样一个好助手。

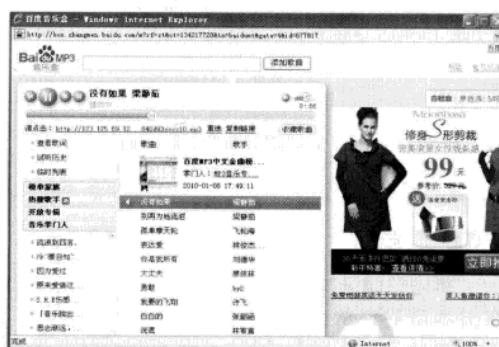
STEP 01 启动影音神探

启动影音神探，打开其运行窗口，如下图所示。



STEP 02 输入 ftp 服务器地址

单击“开始嗅探”按钮，然后打开一个带有音频或图片的网页，如下图所示。



STEP 03 显示捕获文件相应信息

此时影音神探工作窗口中的列表中将显示出所捕获文件的相应信息，音频或视频文件会以红色形式标示出来，如下图所示。



STEP 04 选择“用影音传送带下载”选项

在文件列表中选中需要下载的文件，然后右击，在弹出的快捷菜单中选择“用影音传送带下载”选项，即可下载该文件，如下图所示。



提示

影音神探不仅可以在音乐网站或者影视网站读取影音文件的地址，还可以用于探测某些软件运行后是否会下载后门文件。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter

03

Windows 系统漏洞攻防

Windows 是目前应用最为广泛的操作系统，但它并非想象中的那样完美，蓝屏、死机、上网后资料遗失、服务器遭受攻击等问题层出不穷，这些即为“系统漏洞”，黑客经常利用一些系统漏洞对 Windows 操作系统进行入侵。本章将详细介绍有关 Windows 系统漏洞攻防方面的知识。

本章建议学习时间：

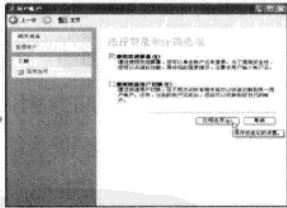
本章建议学习时间为 40 分钟，其中分配 15 分钟学习认识系统漏洞及其产生的原因，以及 Windows 中存在的系统漏洞，25 分钟学习系统漏洞检测与修复知识。

学完本章后您可以：

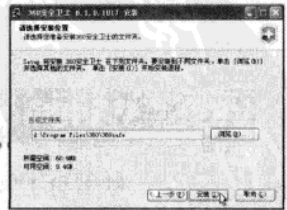
- 了解系统漏洞及其产生原因
- 认识 Windows 中存在的系统漏洞
- 利用 Windows 自动更新软件
- 使用 360 安全卫士修复系统漏洞
- 使用瑞星卡卡修复系统漏洞



选择 UPNP 服务项



启用屏幕密码保护



设置扫描范围



重要知识点视频索引



3.1 认识系统漏洞

Windows 操作系统系列是当今使用最为广泛的操作系统，随着技术的不断进步，它们的安全性能越来越高，但其系统漏洞依然层出不穷。

3.1.1 什么是系统漏洞

系统漏洞往往是伴随操作系统而产生的，有了操作系统也就有了系统漏洞，并在操作系统的生命周期内一直存在。

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，这些缺陷或错误可以被不法者或电脑黑客利用，通过植入木马、病毒等方式来攻击或控制整个电脑，从而窃取用户电脑中的重要资料和信息，甚至破坏用户的操作系统，让系统瘫痪。

3.1.2 系统漏洞产生的原因

系统漏洞的产生不是安装不当的结果，也不是使用后的结果，而是编程者在程序编写过程中为了实现不可告人的目的，在程序代码的隐蔽处保留的后门。另一方面它受编程人员的能力、经验和当时安全技术所限，在程序中难免会有不足之处，轻则影响程序效率，重则导致非授权用户的权限提升。

Windows 操作系统可以说是现在个人计算机上使用最为广泛的操作系统，从最初的 DOS 1.0 到现在的 Windows 7，微软公司为我们提供了一个越来越稳定、使用越来越方便的操作系统。但微软的程序员并不是神，Windows 庞大的构架特性，使得他们在设计或编写程序时难免会出现错误，从而使操作系统中存在着诸多的安全漏洞。系统漏洞产生的原因归结起来，主要有以下几点：

1. 人为因素

编程人员在编写程序过程中为了某些不可告人的目的，故意在程序代码的隐蔽位置保留了后门。

2. 硬件因素

因为硬件的原因，编程人员无法弥补硬件的漏洞，从而使硬件问题通过软件表现出来。

3. 客观因素

受编程人员的能力、经验和当时的安全技术及加密方法所限，在程序中难免存在不足之处，而这些不足恰恰会导致系统漏洞的产生。

系统漏洞虽然大量存在，但只要我们平时多了解操作系统的各种漏洞、黑客的工具手段以及防御的方法，及时对系统进行更新，安装好系统修补程序，基本上可以保护自己系统的安全。

3.2 Windows 中存在的系统漏洞

随着技术的不断进步，Windows 操作系统的安全性能也越来越高。下面将主要对 Windows XP 中存在的系统漏洞进行简单介绍，希望读者通过对这些系统漏洞的了解，能够提高自身的防范意识。

Chapter 03 Windows 系统漏洞攻防

同以前的操作系统相比，Windows XP 具有更加安全和更加保密的安全特性，其基于 Windows 2000 的安全设计大大提高了用户建立安全、保密的系统环境的系数，但其同样存在着大量的安全漏洞。

Work1 升级程序漏洞

例如，将 Windows XP 升级至 Windows XP Pro，IE 6.0 浏览器即会重新安装，以前的补丁程序将被全部清除。

Windows XP 的升级程序不仅会删除 IE 浏览器的补丁文件，还会导致微软的升级服务器无法正确识别 IE 是否存在缺陷，即 Windows XP Pro 系统存在两个潜在威胁：

- ❖ 某些网页或 HTML 邮件的脚本可自动调用 Windows 的程序。
- ❖ 可通过 IE 漏洞窥视用户的计算机文件。

解决方法：

如果 IE 浏览器未下载升级补丁，可到微软官方网站下载最新的补丁程序。

Work2 帮助和支持中心漏洞

帮助和支持中心提供集成工具，用户通过该工具获取针对各种主题的帮助和支持。目前版本的 Windows XP 帮助和支持中心存在漏洞，该漏洞使攻击者可跳过特殊的网页（在打开该网页时，调用错误的函数，并将存在的文件或文件夹的名字作为参数传送）来使上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。

该漏洞除使攻击者可删除文件外，不会赋予其他权利，攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

解决方法：

安装 Windows XP 的 Service pack 1 补丁。

Work3 压缩文件夹漏洞

Windows XP 压缩文件夹可按攻击者的选择运行代码。在安装“Plus!”包的 Windows XP 系统中，“压缩文件夹”功能允许将 Zip 文件作为普通文件夹处理。“压缩文件夹”功能存在两个漏洞，具体如下：

- ❖ 在解压缩 Zip 文件时会有未经检查的缓冲存在于程序中以存放被解压文件，因此很可能导致浏览器崩溃或攻击者的代码被运行。
- ❖ 解压缩功能在非用户指定目录中放置文件，可使攻击者在用户系统的已知位置放置文件。

解决方法：

不接收不信任的邮件附件，也不下载不信任的文件。

Work4 UPNP 服务漏洞

Windows XP 默认启动的 UPNP 服务存在严重安全漏洞。UPNP (Universal Plug and Play) 体系面向无线设备、PC 和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备间提供 TCP/IP 连接和 Web 访问功能，该服务可用于检测和集成 UPNP 硬件。

基础
知识

常用
扫描
与嗅探
工具

Windows
系统
漏洞
攻防

设置
系统
安全
策略

系统
与文
件加
密

远程
控制
攻防

木马
攻防

聊天
软件
攻防

网页
恶意
代码
攻防

电子
邮件
攻防

病毒
攻防

使用
电脑
安全
软件

黑客
攻防
实用
技巧



UPNP 协议存在安全漏洞，使攻击者可非法获取任何 Windows XP 的系统级访问并进行攻击，还可以通过控制多台安装 Windows XP 的电脑发起分布式的攻击。

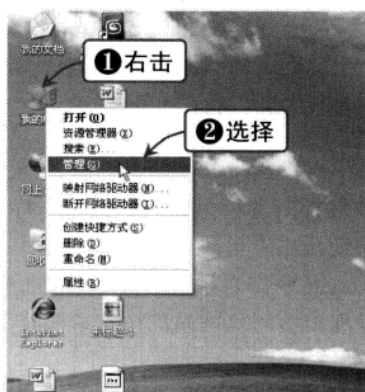
解决方法：

- (1) 建议禁用 UPNP 服务。
- (2) 在官方网站下载补丁程序。

禁用 UPNP 服务的具体操作方法如下：

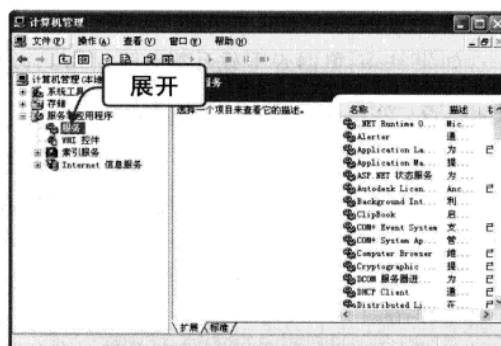
STEP 01 选择“管理”选项

在“我的电脑”图标上右击，在弹出的快捷菜单中选择“管理”选项，如下图所示。



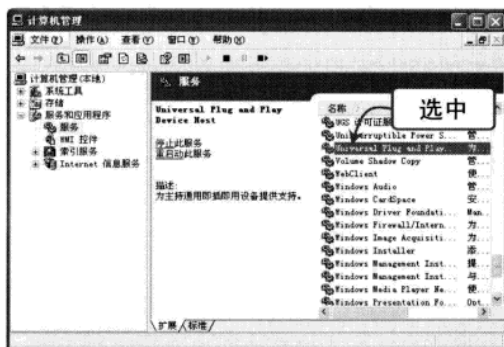
STEP 02 打开“计算机管理”窗口

打开“计算机管理”窗口，在左侧窗格中依次展开“计算机管理（本地）”|“服务和应用程序”|“服务”选项，如下图所示。



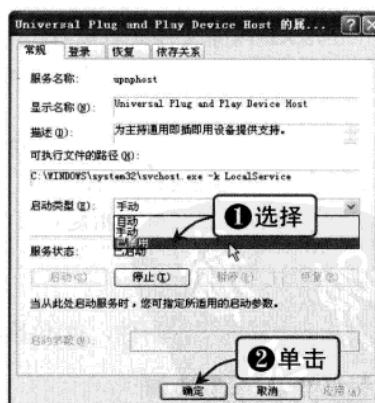
STEP 03 选择 UPNP 服务项

在右侧窗格中选中的 Universal Plug and Play Device Host 服务项（如下图所示），双击该服务项，打开“Universal Plug and Play Device Host 的属性”对话框。



STEP 04 禁用 UPNP 服务

在“启动类型”下拉列表框中选择“已禁用”选项（如下图所示），单击“确定”按钮即可禁用 UPNP 服务。



Work5 服务拒绝漏洞

Windows XP 支持点对点的协议（PPTP），是作为远程访问服务实现的虚拟专用网技术，由于在用于控制建立、维护和拆开 PPTP 连接的代码段中存在未经检查的缓存，导致 Windows XP

Chapter 03 Windows 系统漏洞攻防

的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的 PPTP 控制数据，攻击者可损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。

该漏洞可攻击任何一台提供 PPTP 服务的服务器，对于 PPTP 客户端的工作站，攻击者只需激活 PPTP 会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。

解决方法：

建议不默认启动 PPTP。

Work6 VM 漏洞

VM 漏洞可能造成信息泄露，并执行攻击者的代码。攻击者可通过向 JDBC 类传送无效的参数使宿主应用程序崩溃，攻击者需在网站上拥有恶意的 Java applet 并引诱用户访问该站点。

恶意用户可在用户机器上安装任意 DLL，并执行任意的本机代码，隐蔽地破坏或读取内存数据。

解决方法：

建议经常进行相关软件的安全更新。

Work7 Windows Media Player 漏洞

Windows Media Player 漏洞可能导致用户信息的泄露、脚本调用以及缓存路径泄露。Windows Media Player 漏洞主要产生两个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法，微软对其定义的严重级别为“严重”；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难，它的严重级别也就比较低。

解决方法：

Windows Media Player 的信息泄漏漏洞不会影响在本地机器上打开的媒体文件。因此，建议将要播放的文件先下载到本地再播放，即可不受利用此漏洞进行的攻击。脚本执行漏洞仅有完全按下面的顺序进行一系列操作，攻击者才可能利用该漏洞进行一次成功攻击，否则攻击将不会成功。具体的操作如下：用户必须播放位于攻击者那边的一个特殊的媒体文件；播放该特殊文件后，该用户必须关闭 Windows Media Player 而不再播放其他文件；用户必须接着浏览一个由攻击者构建的网页。因此，只需用户不按照该顺序进行操作，即可不受攻击。

Work8 RDP 漏洞

Windows 操作系统通过 RDP（remote data protocol）为客户端提供远程终端会话。RDP 协议将终端会话的相关硬件信息传送到远程客户端，其漏洞如下：

（1）与某些 RDP 版本的会话加密实现有关的漏洞

所有 RDP 实现均允许对 RDP 会话中的数据加密，然而在 Windows 2000 和 Windows XP 版本中，纯文本会话数据的校验在发送前并未经过加密，窃听并记录 RDP 会话的攻击者可对该校验密码分析攻击并覆盖该会话传输。

（2）与 Windows XP 中的 RDP 实现对某些不正确的数据包处理方法有关的漏洞

当接收这些数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者向

黑客
基础
与
常用
扫描
工具
Windows
系统
漏洞
攻防
设置
系统
安全
策略
系统
与
文
件
加
密
远程
控
制
攻
防
木
马
聊
天
软
件
攻
防
网
页
恶
意
攻
防
电
子
邮
件
攻
防
C
盘
病
毒
攻
防
使
用
电
脑
安
全
软
件
黑
客
攻
防
技
巧



一个已受影响的系统发送这类数据包时，并不需经过系统验证。

解决方法：

Windows XP 默认并未启动它的远程桌面服务，即使远程桌面服务启动，只需在防火墙中屏蔽 3389 端口，即可避免该攻击。

远程桌面服务即 Terminal Services 服务，禁用此服务的具体操作方法如下：

STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，如下图所示。



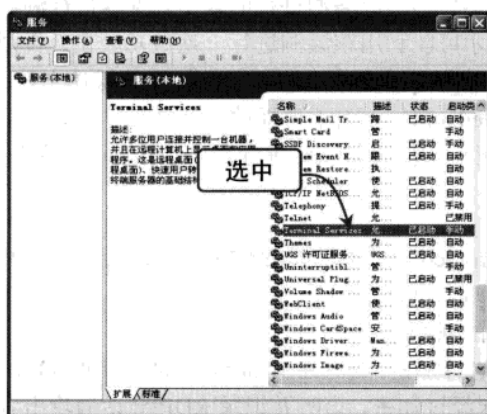
STEP 02 打开“管理工具”窗口

在“控制面板”窗口中双击“管理工具”图标，打开“管理工具”窗口，如下图所示。



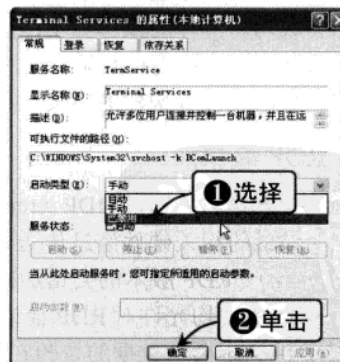
STEP 03 打开“服务”窗口

双击“管理工具”窗口中的“服务”图标，打开“服务”窗口，在其右侧的窗格中选中 Terminal Services 服务，如下图所示。



STEP 04 禁用远程桌面服务

双击 Terminal Services 服务项，打开“Terminal Services 的属性（本地计算机）”对话框，在“启动类型”下拉列表框中选择“已禁用”选项（如下图所示），单击“确定”按钮，即可禁用远程桌面服务。



Work9 热键漏洞

设置热键后，由于 Windows XP 的自注销功能可使系统“假注销”，其他用户即可通过

Chapter 03 Windows 系统漏洞攻防

热键调用程序。

热键功能是系统提供的服务，当用户离开电脑后，该电脑即处于未保护情况下，此时 Windows XP 会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，仍可使用热键启动应用程序。

解决方法：

❖ 由于该漏洞被利用的前提为热键可用，因此需检查可能会带来危害的程序和服务的热键。

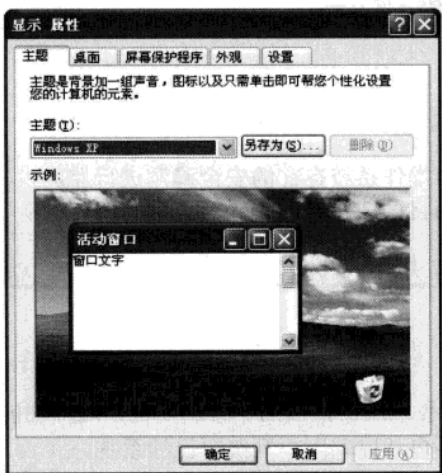
❖ 启动屏幕保护程序，并设置密码。

❖ 建议在离开电脑时锁定电脑。

启用屏幕保护程序的具体操作步骤如下：

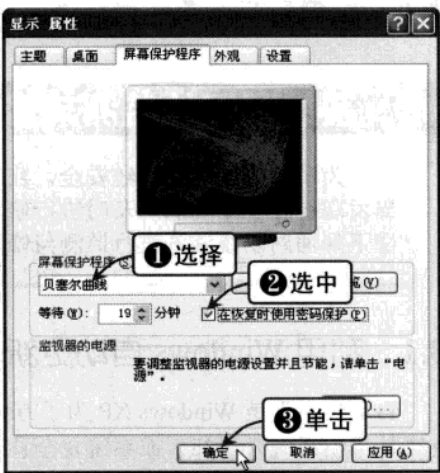
STEP 01 打开“显示 属性”对话框

在桌面空白位置右击，在弹出的快捷菜单中选择“属性”选项，打开“显示 属性”对话框，如下图所示。



STEP 02 启用屏幕密码保护

选择“屏幕保护程序”选项卡，在“屏幕保护程序”下拉列表框中选择一种屏保方式，并选中“在恢复时使用密码保护”复选框（如下图所示），然后单击“确定”按钮即可。



Work10 账号快速切换漏洞

Windows XP 快速账号切换功能存在问题，可造成账号锁定，使所有非管理员账号均无法登录。

Windows XP 设计了账号快速切换功能，使用户可快速地在不同的账号间切换，但其设计存在问题。当用户利用账号快速切换功能快速重试登录另一个用户名时，系统会判别为暴力破解，从而导致非管理员账号锁定，使所有非管理员账号均无法登录。

解决方法：

暂时禁止账户快速切换功能。

禁止账户快速切换功能的具体操作方法如下：

基础
知识

常用
扫描
与嗅探
工具

Windows
系统
漏洞
攻防

设置
系统
安全
策略

系统
与文
件加
密

远程
控
制
攻
防

木
马
攻
防

聊
天
软
件
攻
防

网
页
恶
意
代
码
攻
防

电
子
邮
件
攻
防

已
知
漏
洞
攻
防

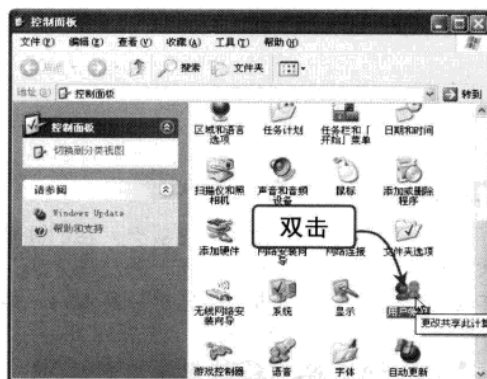
使用
电
脑
安
全
软
件

黑
客
攻
防
实
用
技
巧



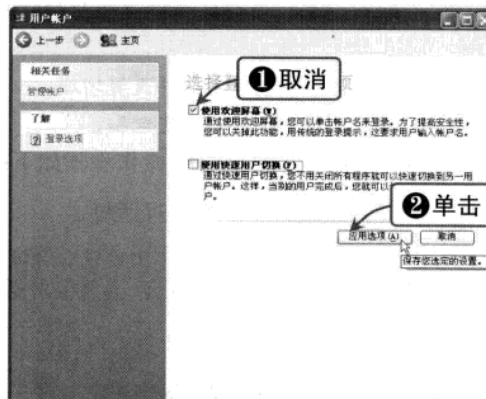
STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“用户账户”图标，如下图所示。



STEP 02 完成设置

打开“用户账户”窗口，单击“更改用户登录或注销的方式”超链接，然后在弹出的窗口中取消选择“使用快速用户切换”复选框，并单击“应用选项”按钮，如下图所示。



3.3 系统漏洞的监测与修复

为了有效地保护系统安全，我们需要对操作系统存在的安全漏洞进行监测，当发现存在安全漏洞时及时进行修复。下面将详细讲解在 Windows XP 系统环境下如何对系统漏洞进行监测与修复。

3.3.1 利用 Windows 自动更新软件

“自动更新”是 Windows XP 为了方便用户升级系统而推出的一种新功能，这种功能可以在微软推出系统升级补丁或系统安全补丁的时候自动提醒用户升级自己的系统。

Work1 启用 Windows 自动更新

要使用 Windows XP 自带的自动更新软件，必须先启用 Windows 自动更新，其具体操作方法如下：

STEP 01 打开“Windows 安全中心”窗口

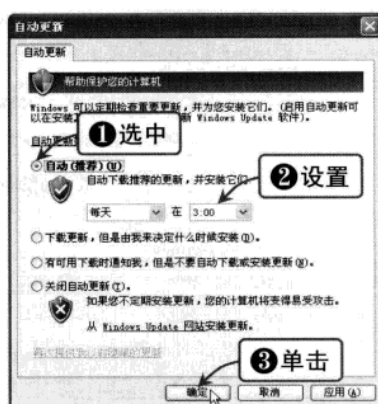
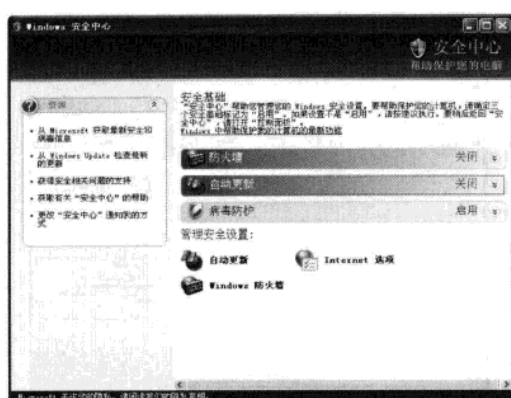
单击“开始”|“所有程序”|“附件”|“系统工具”|“安全中心”命令，打开“Windows 安全中心”窗口，如下图所示。

STEP 02 “自动更新”对话框

单击“自动更新”超链接，在打开的“自动更新”对话框中选中“自动（推荐）”单选按钮，并在下面设置升级频率和时间（如下图所示），然后单击“确定”按钮，即可启用 Windows 自动更新功能。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 03 Windows 系统漏洞攻防



提示

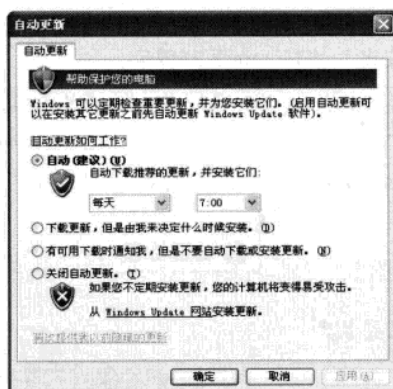
用户如果不想让系统自动更新，可以在“自动更新”对话框中选中“下载更新，但是由我来决定什么时候安装”单选按钮，自己决定安装哪些更新程序。

Work2 从微软官方网站下载更新程序

启用 Windows 自动更新功能后，系统会自动下载当前系统可用的更新程序并进行安装。用户也可以从微软的官方网站下载更新程序，其具体操作步骤如下：

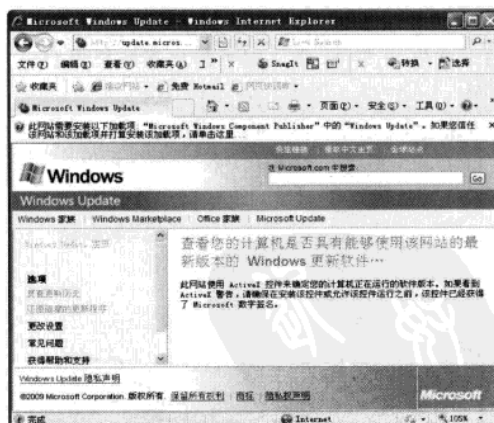
STEP 01 打开“自动更新”对话框

单击“开始”|“所有程序”|“附件”|“系统工具”|“安全中心”命令，打开“Windows 安全中心”窗口，然后单击“自动更新”图标，打开“自动更新”对话框，如下图所示。



STEP 02 打开自动更新页面

单击该窗口下方的“Windows Update 网站”超链接，打开微软官方网站的自动更新页面，如下图所示。



STEP 03 安装 Windows Update 加载项

此时该页面中会显示提示信息，要求用户加载 Windows Update 加载项，安装此加载项后的网页如下图所示。

STEP 04 搜索当前系统需要的更新程序

单击“快速”按钮，开始搜索当前系统需要的更新程序（如下图所示），然后根据网页中的提示开始更新系统程序即可。

黑客
基础知识

常用扫描
与嗅探工具

Windows 系
统漏洞攻防

设置系统
安全策略

系统与文
件加密

远程控
制攻防

木马
攻防

聊天软
件攻防

网页恶
意代码攻防

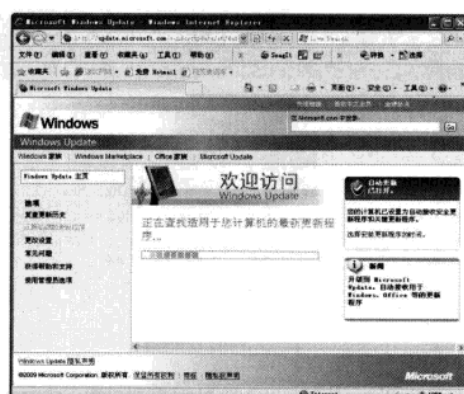
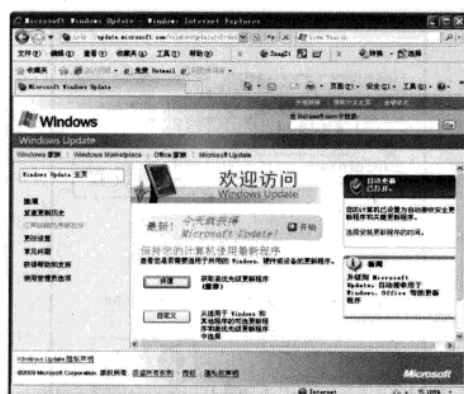
电子邮
件攻防

C 盘病
毒攻防

使用电脑
安全软件

黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



3.3.2 使用 360 安全卫士

如果感觉使用 Windows 自动更新程序比较麻烦，还可以安装 360 安全卫士，由 360 安全卫士自动搜索并安装当前系统的安全补丁程序。

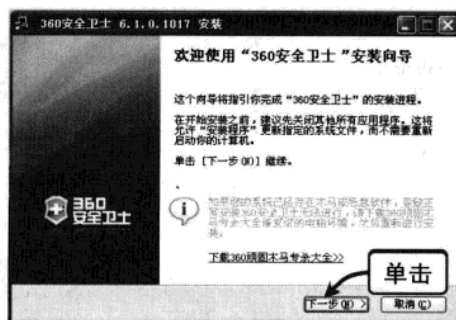
360 安全卫士是一款免费的上网安全软件，它使用方便，拥有木马查杀、恶意软件清理、漏洞补丁修复、电脑全面体检等多种功能，倍受用户欢迎。另外，360 安全卫士还具备开机加速、垃圾清理等多种系统优化功能，可大大加快电脑运行速度，内含的 360 软件管家还可以帮助用户轻松下载、升级和强力卸载各种应用软件。

Work1 安装 360 安全卫士

从 360 安全中心网站首页下载 360 安全卫士的网络安装程序，即可开始安装 360 安全卫士，其具体操作步骤如下：

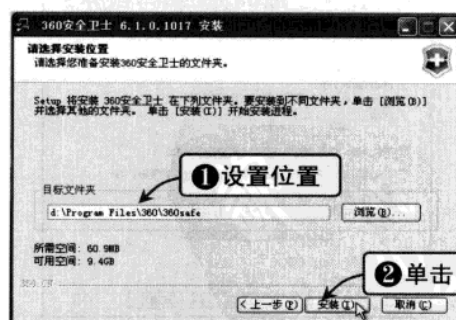
STEP 01 打开安装程序窗口

双击 360 安全卫士安装程序图标，系统开始下载安装文件，稍后即可弹出安装程序窗口，单击“下一步”按钮，如下图所示。



STEP 02 设置扫描范围

在弹出的用户许可协议界面单击“我接受”按钮，在弹出的界面中设置程序安装位置，单击“安装”按钮，如下图所示。



STEP 03 输入 netstat -a -n 命令

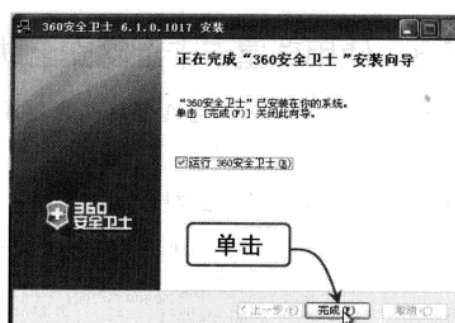
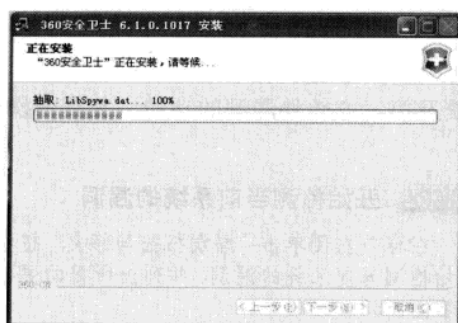
开始安装程序，如下图所示。

STEP 04 查看端口状态

安装完毕后，在弹出的窗口中直接单击“下一步”按钮继续，在如下图所示的窗口中单击“完成”按钮，即可完成安装。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 03 Windows 系统漏洞攻防

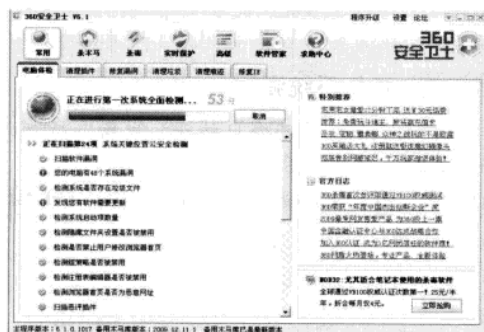


Work2 修补系统漏洞

利用 360 安全卫士可以自动检测当前系统存在的安全漏洞，并快速下载针对这些安全漏洞的补丁程序进行安装，其具体操作步骤如下：

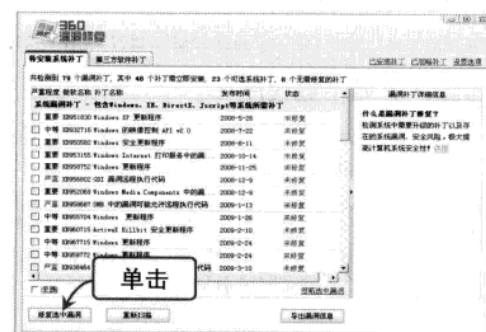
STEP 01 打开 360 安全卫士程序主界面

双击 360 安全卫士程序图标，打开 360 安全卫士程序主界面，软件会自动检测当前系统安全性能，并对其进行评分，如下图所示。



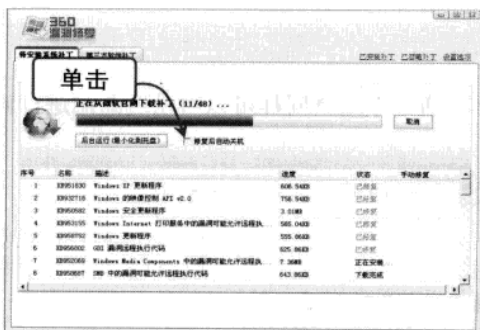
STEP 02 检测系统中存在的系统漏洞

单击“修复漏洞”按钮，打开“360 漏洞修复”窗口，软件会自动检测系统中存在的系统漏洞和需要升级的补丁程序，如下图所示。



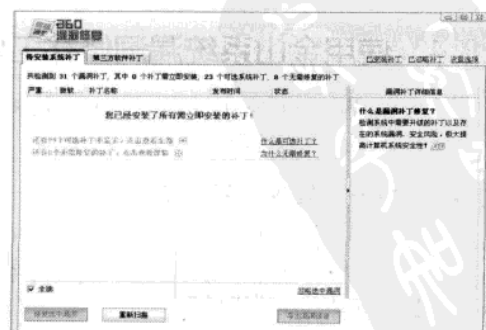
STEP 03 下载补丁程序并进行安装

选中窗口下方的“全选”复选框，将检测到的系统漏洞和升级补丁全部选中，单击“修复选中漏洞”按钮，开始下载补丁程序并进行安装，如下图所示。



STEP 04 安装完毕所有所需的系统补丁

当系统补丁程序安装完毕后，将弹出如下图所示的提示信息，用户还可以对其他可选补丁进行安装。



基础知识

与嗅探工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制

木马攻击

聊天软件攻击

网页恶意代码攻击

电子邮件攻击

病毒攻击

使用电脑安全软件

黑客攻防

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



3.3.3 使用瑞星卡卡上网安全助手

瑞星卡卡上网助手也具有自动修复操作系统及第三方软件漏洞的功能，其具体操作步骤如下：

STEP 01 打开瑞星卡卡上网安全助手

单击瑞星卡卡上网安全助手程序图标，打开其主工作界面，如下图所示。



STEP 02 开始检测当前系统的漏洞

在窗口左侧单击“漏洞扫描与修复”按钮，开始检测当前系统的漏洞，并列出所需的更新，如下图所示。



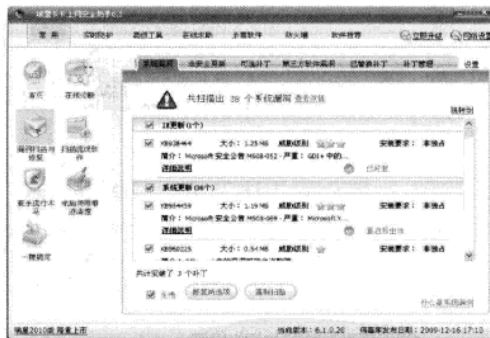
STEP 03 开始下载程序

选中“全选”复选框，单击“修复所选选项”按钮，开始下载程序，如下图所示。



STEP 04 修复系统漏洞

下载完毕后系统会自动安装更新，所选系统漏洞修复完后会给出提示，如下图所示。



3.3.4 使用金山系统漏洞修补工具

金山系统清理专家集成有系统漏洞修补工具，通过该工具同样可以对系统漏洞进行修复，其具体操作步骤如下：

STEP 01 打开“管理工具”窗口

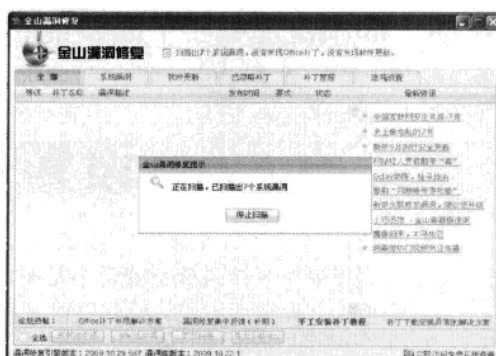
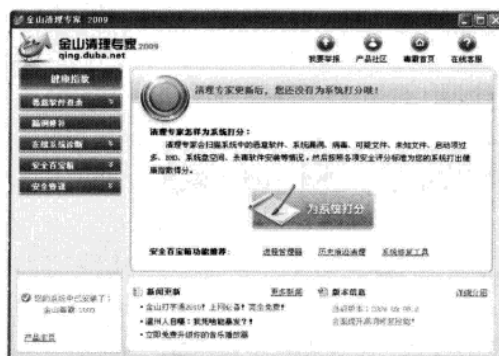
安装金山毒霸组件后，双击桌面上的“金山系统清理专家”图标，打开“金山系统清理专家 2009”程序窗口，如下图所示。

STEP 02 扫描现有的系统漏洞

在“金山系统清理专家 2009”程序窗口左侧单击“漏洞修补”选项卡，开始扫描现有的系统漏洞，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 03 Windows 系统漏洞攻防

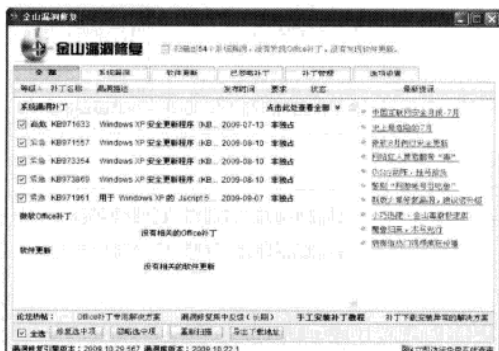


提示

对于扫描出的系统漏洞，金山漏洞修复工具会自动对其进行分类，其中有高危和紧急的系统漏洞，还有 Office 补丁和软件更新程序。

STEP 03 创建 IP 安全策略

扫描完毕后窗口中会将高度危险和紧急的系统漏洞显示出来，如下图所示。



STEP 04 IP 安全策略向导

选中“全选”复选框，单击“修复选中项”按钮，对这些系统漏洞进行修复，如下图所示。



基础知识

与嗅探工具

Windows 系统

安全策略

系统与安全

远程控制

攻防

聊天软件

网页恶意

代码攻防

电子邮件

攻击

攻击

攻击

Chapter

04

设置系统安全策略

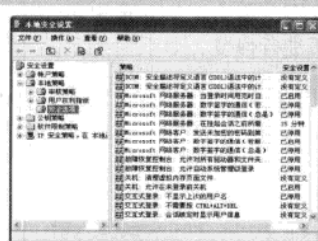
其实很多时候系统不安全不是操作系统或安全软件存在问题，而是用户对系统安全设置不了解，没有设置正确的系统安全策略，从而给了黑客可乘之机。本章将通过设置本地安全策略、设置组策略、设置计算机管理策略和注册表编辑器安全防范等操作，详细介绍系统安全策略设置的相关知识。

本章建议学习时间：

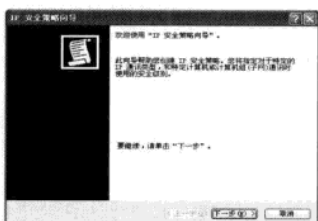
本章建议学习时间为 60 分钟，其中分配 20 分钟学习如何设置本地安全策略，15 分钟学习如何设置组策略，10 分钟学习如何设置计算机管理策略，15 分钟学习如何设置注册表编辑器。

学完本章后您可以：

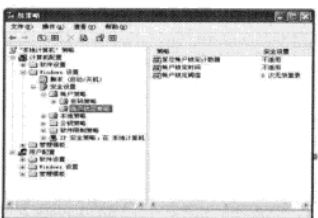
- 设置本地安全策略
- 设置组策略
- 设置计算机管理策略
- 注册表编辑器安全防范



打开“本地安全设置”窗口



打开“IP 安全策略向导”对话框



选择“账户锁定策略”选项

重要知识点视频索引



4.1 设置本地安全策略

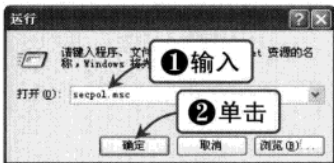
Windows XP 系统自带的“本地安全策略”是一个很不错的系统安全管理工具，利用它我们可以使自己的操作系统更加安全。下面将具体讲解设置本地安全策略的各种方法。

4.1.1 禁止在登录前关机

在工作中如果需要暂时离开，可以按【Windows+L】组合键来锁定计算机，回来后只需输入登录密码即可继续工作。但在锁定界面中有一个“关闭计算机”选项，为了防止他人关闭计算机，可以通过启用“禁止在登录前关机”安全策略来实现。

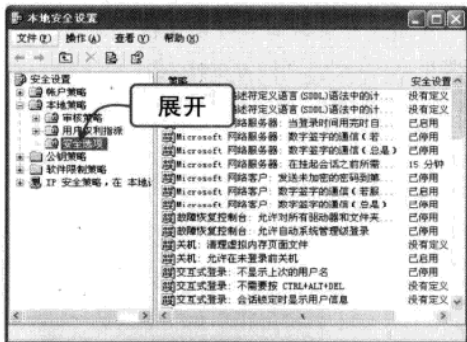
STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，打开“运行”对话框，然后在“打开”下拉列表框中输入命令 secpol.msc，单击“确定”按钮，如下图所示。



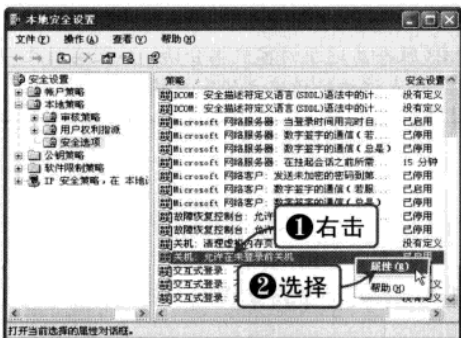
STEP 02 打开“本地安全设置”窗口

打开“本地安全设置”窗口，然后在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，如下图所示。



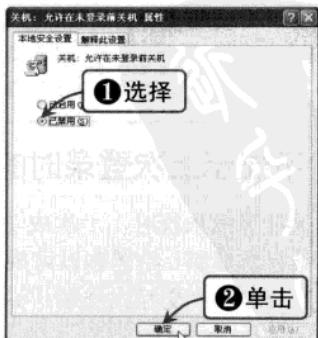
STEP 03 选择“属性”选项

在右侧窗格中找到“关机：允许在未登录前关机”选项，在该选项上右击，在弹出的快捷菜单中选择“属性”选项，如下图所示。



STEP 04 禁用该服务项

打开“关机：允许在未登录前关机 属性”对话框，在该对话框中选中“已禁用”单选按钮，然后依次单击“应用”和“确定”按钮（如下图所示），即可完成设置。





提示

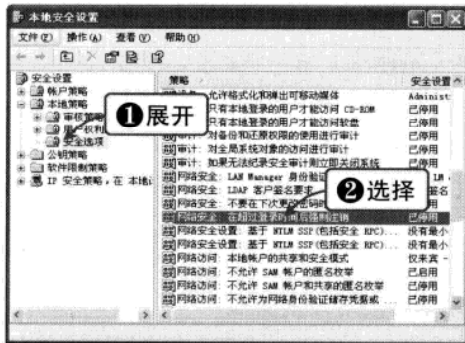
“禁止在登录前关机”安全策略选项用来确定是否可以在无需登录到 Windows 的情况下关闭计算机。启用此策略时，Windows 登录屏幕上的“关机”命令可用。禁用此策略时，Windows 登录屏幕上不会显示关闭计算机选项。在这种情况下，用户必须能够成功登录到计算机并具有关闭系统的用户权限，然后才可以执行关闭系统的操作。

4.1.2 在超过登录时间后强制用户注销

当某些用户连接到本地计算机上且已经超过有效登录时间时，需要让计算机自动断开与该用户的连接，利用“网络安全：在超过登录时间后强制注销”选项可以解决这一问题，其具体设置方法如下：

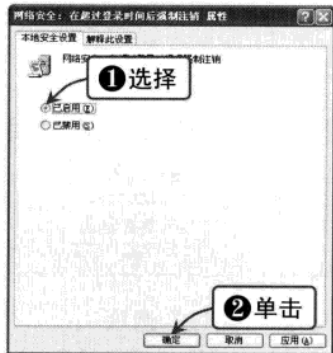
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧窗格中找到“网络安全：在超过登录时间后强制注销”选项，如下图所示。



STEP 02 完成设置

双击该选项，打开“网络安全：在超过登录时间后强制注销 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“应用”和“确定”按钮即可应用设置。



提示

“网络安全：在超过登录时间后强制注销”安全策略选项用于确定在连接到本地计算机的用户超出其用户账户的有效登录时间时，是否断开与其的连接。此设置会影响服务器消息块（SMB）组件。启用此策略时，一旦客户端的登录时间过期，该策略便会强制断开与 SMB 服务器建立的客户端会话。如果禁用此策略，即便在客户端登录时间过期后，仍允许维持已建立的客户端会话。

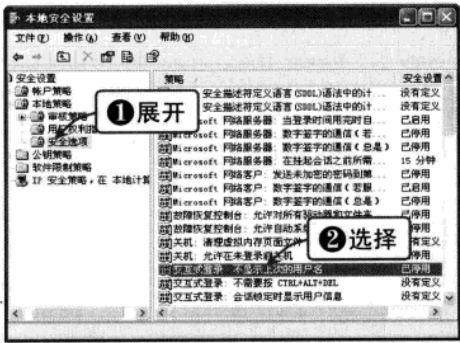
4.1.3 不显示上次登录时的用户名

在登录计算机系统时，上次成功登录的用户名会显示在 Windows 登录界面上，这可能造成账户信息的泄露，给黑客以可乘之机。为了让上次成功登录的用户名在登录界面不再显示，可以通过启用“交互式登录：不显示上次用户名”安全策略来实现，其具体操作步骤如下：

Chapter 04 设置系统安全策略

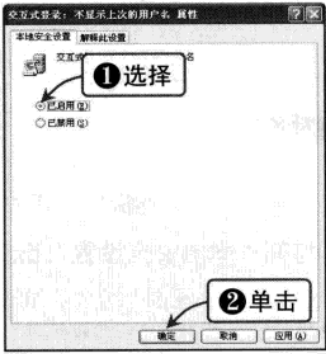
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全策略”选项，然后在右侧窗格中找到“交互式登录：不显示上次的用户名”选项，如下图所示。



STEP 02 完成设置

双击该选项，打开“交互式登录：不显示上次的用户名 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“应用”和“确定”按钮即可应用设置。



提示

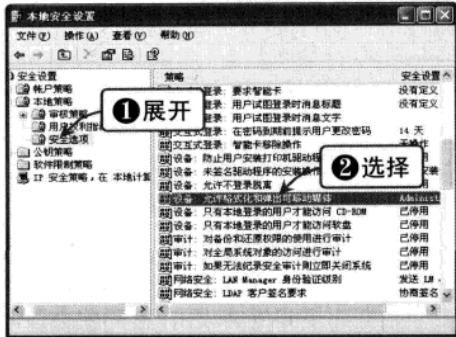
“交互式登录：不显示上次的用户名”安全策略选项用于确定是否在 Windows 登录屏幕中显示最后登录到计算机的用户的名称。如果启用该策略，则不会在“登录到 Windows”对话框中显示最后成功登录的用户的名称；如果禁用该策略，则会显示最后登录的用户的名称。

4.1.4 限制格式化和弹出可移动媒体

如果系统允许格式化和弹出可移动媒体，黑客可以从一台计算机中读取媒体文件，然后通过另一台具有本地管理员特权的计算机访问此媒体文件。为了避免出现上述现象，可以禁用“设备：允许格式化和弹出可移动媒体”安全策略，其具体操作步骤如下：

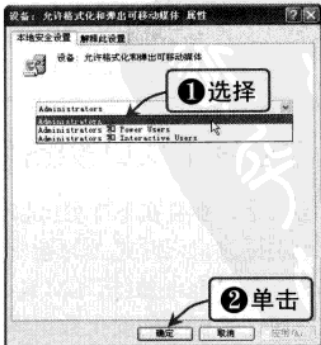
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全策略”选项，然后在右侧窗格中找到“设备：允许格式化和弹出可移动媒体”选项，如下图所示。

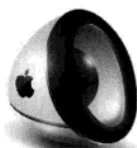


STEP 02 查看 IP 地址所属地区

双击该选项，打开“设备：允许格式化和弹出可移动媒体 属性”对话框，在该对话框中设置允许执行此操作的用户（如下图所示），然后单击“应用”和“确定”按钮即可应用设置。



基础知识
黑客
常用扫描
与嗅探工具
系统漏洞
安全策略
系统设置
系统安全
系统加密
远程控制
木马
聊天软件
网页病毒
代码攻击
电子邮件
C盘病毒
使用电脑
安全软件
黑客技巧



提示

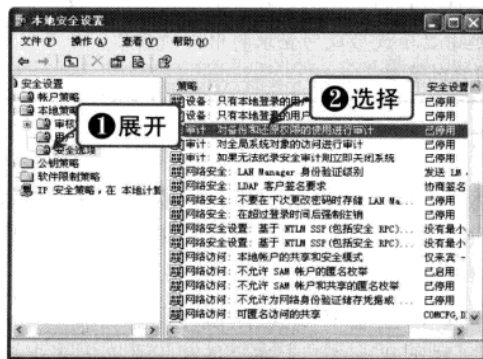
“设备：允许格式化和弹出可移动媒体”安全策略选项用于确定允许格式化和弹出可移动 NTFS 介质的用户，可以将此功能授予：Administrators、Administrators 和 Power Users、Administrators 和 Interactive Users。

4.1.5 对备份和还原权限进行审计

启用对备份和还原权限进行审计功能，可以将所有实施用户权限的实例都记录到安全日志中，用户可以通过在“本地安全设置”窗口中启用“审计：对备份和还原权限的使用进行审计”安全策略，其具体操作步骤如下：

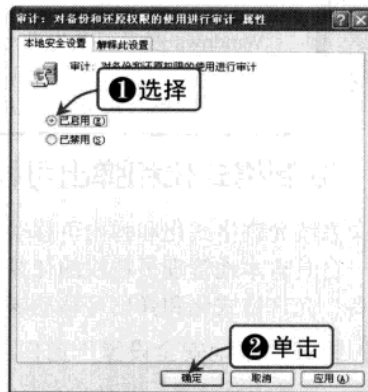
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全策略”选项，然后在右侧窗格中找到“审计：对备份和还原权限的使用进行审计”选项，如下图所示。



STEP 02 完成设置

双击该选项，打开“审计：对备份和还原权限的使用进行审计 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“应用”和“确定”按钮即可应用设置。



提示

“审计：对备份和还原权限的使用进行审计”安全策略选项用于确定当审核权限使用策略生效时，是否审核包括备份和还原在内的所有用户权限的使用。启用审核权限使用策略的同时启用此选项，会为备份或还原的每个文件生成一个审核事件。如果禁用此策略，则即使启用了审核权限使用时，也不会审核备份或还原权限的使用。

4.1.6 禁止在下次更改密码时存储 LAN Manager 的 Hash 值

“网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值”安全策略选项用于确定在下次更改密码时是否为新密码存储 LAN Manager (LM) 的 Hash 值。相比加密性更强的 Windows NT Hash 算法，LM Hash 值的加密性相对较弱，易于遭受攻击。由于 LM Hash 值存储在本地计算机上的安全数据库中，因此一旦安全数据库受到黑客攻击，密码便会泄漏。

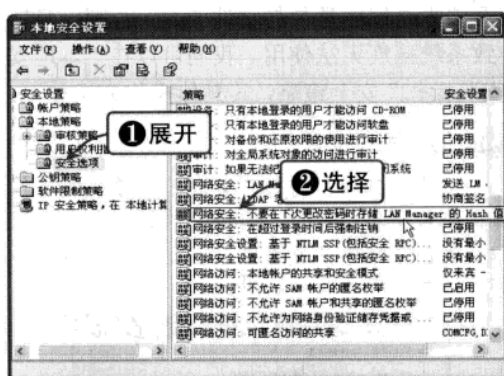
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 04 设置系统安全策略

禁止在下次更改密码时存储 LAN Manager Hash 值的具体操作方法如下:

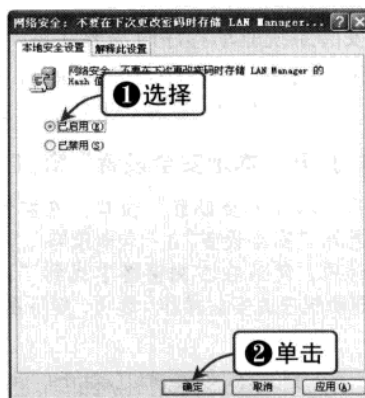
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧窗格中找到“网络安全：不要在下次更改密码时存储 LAN Manager 的 Hash 值”选项，如下图所示。



STEP 02 完成设置

双击该选项, 打开“网络安全: 不要在下次更改密码时存储 LAN Manager 的 Hash 值 属性”对话框, 选中“已启用”单选按钮 (如下图所示), 然后单击“应用”和“确定”按钮即可应用设置。

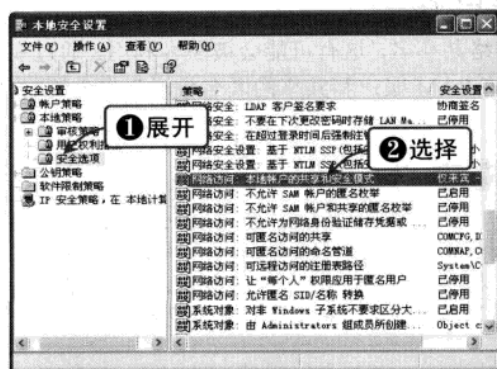


4.1.7 设置本地账户共享与安全模式

在使用网络共享时,为了保护用户信息的安全,需要对本地账户的网络登录进行身份验证,我们可以通过设置“本地安全设置”窗口中的“网络访问:设置本地账户的共享和安全模式”安全策略来实现,其具体操作步骤如下:

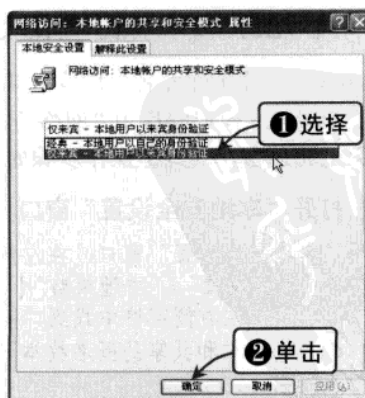
STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧窗格中找到“网络访问：设置本地账户的共享和安全模式”选项，如下图所示。



STEP 02 完成设置

双击该选项，打开“网络访问：设置本地账户的共享和安全模式 属性”对话框，在该对话框的下拉列表框中选择合适的选项，然后单击“应用”和“确定”按钮即可应用设置。





提示

“网络访问：设置本地账户的共享和安全模式”安全策略选项用于确定如何对使用本地账户的网络登录进行身份验证，有两种模式可供我们选择，经典：对本地用户进行身份验证，不改变其本来身份；仅来宾：对本地用户进行身份验证，其身份为来宾。

4.1.8 禁止安装未签名的驱动程序

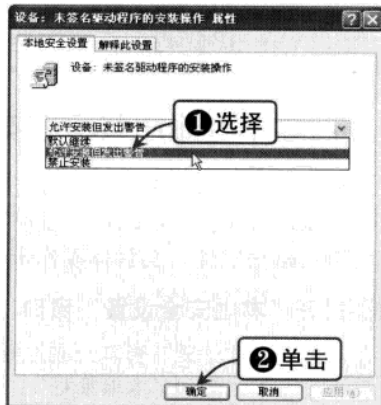
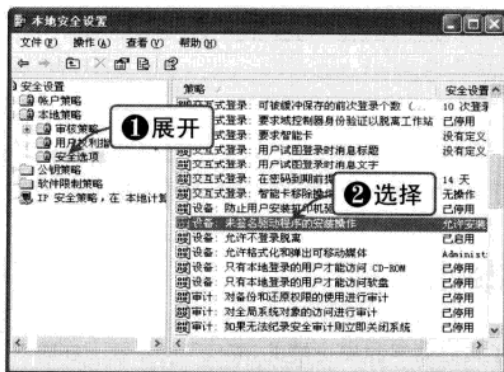
在安装系统驱动程序时需要注意，一定要查看该驱动程序是否与硬件兼容，否则一旦所安装的未签名的驱动程序与硬件冲突，很可能导致系统瘫痪无法使用。我们可以在“本地安全设置”窗口中设置“设备：未签名驱动程序的安装操作”安全策略，其具体操作方法如下：

STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧窗格中找到“设备：未签名驱动程序的安装操作”选项，如下图所示。

STEP 02 完成设置

双击该选项，打开“设备：未签名驱动程序的安装操作 属性”对话框，在该对话框的下拉列表框中选择合适的选项，然后单击“应用”和“确定”按钮即可应用设置。



4.1.9 不允许 SAM 账户和共享的匿名枚举

Windows 系统允许匿名用户枚举域账户和网络共享名，这有可能会被黑客利用，通过在“本地安全设置”窗口中启用“网络访问：不允许 SAM 账户和共享的匿名枚举”安全策略，可以避免上述危害，其具体操作步骤如下：

STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧窗格中找到“网络访问：不允许 SAM 账户和共享的匿名枚举”选项，如下图所示。

STEP 02 完成设置

双击该选项，打开“网络访问：不允许 SAM 账户和共享的匿名枚举 属性”对话框，在该对话框中选中“已启用”单选按钮，然后单击“应用”和“确定”按钮即可应用设置。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 04 设置系统安全策略

1 展开

2 选择

1 选择

2 单击

提示

“网络访问：不允许 SAM 账户和共享的匿名枚举”安全策略选项用于确定是否允许 SAM 账户和共享的匿名枚举。Windows 允许匿名用户执行某些活动，如枚举域账户和网络共享的名称，这很方便，例如，当管理员希望将访问权限授予不维护相互信任的受信任域中的用户时，如果不希望允许 SAM 账户和共享的匿名枚举，可启用此策略。

4.1.10 让“每个人”权限应用于匿名用户

“网络访问：让‘每个人’权限应用于匿名用户”安全策略选项用于确定将哪些附加权限授予连接到计算机的匿名连接。系统默认情况下，Everyone 安全标识符（SID）会从为匿名连接创建的令牌中删除。因此，授予 Everyone 组的权限不会应用于匿名用户。如果启用此策略，会将 Everyone SID 添加到为匿名连接创建的令牌，这样匿名用户就可以访问 Everyone 组拥有权限的所有资源。为防止出现上述情况，可以将此安全策略禁用，其具体操作步骤如下：

STEP 01 打开“本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次展开“安全设置”|“本地策略”|“安全策略”选项，然后在右侧窗格中找到“网络访问：让‘每个人’权限应用于匿名用户”选项，如下图所示。

STEP 02 完成设置

双击该选项，打开“网络访问：让‘每个人’权限应用于匿名用户 属性”对话框，在该对话框中选中“已禁用”单选按钮，然后单击“应用”和“确定”按钮即可应用设置。

基础入门

黑客入门

常用扫描工具

系统漏洞攻防

设置系统安全策略

系统与文档加密

远程控制

木马攻防

聊天软件攻防

网页恶意代码攻防

电子邮箱攻防

病毒攻防

使用电脑安全软件

黑客攻防技巧

81

溜客安全网 WwW.176Ku.CoM



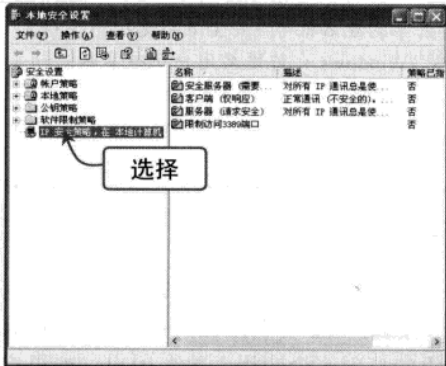
4.1.11 定义 IP 安全策略

创建并定义适合自己的 IP 安全策略，可以为自己的计算机系统提供一个更加安全的操作环境。将一些比较敏感的端口添加到禁止策略中，可以有效地将一些木马、后门程序及网络工具阻隔在系统大门之外。

下面以禁止 23 端口为例，介绍定义 IP 安全策略的方法，其具体操作步骤如下：

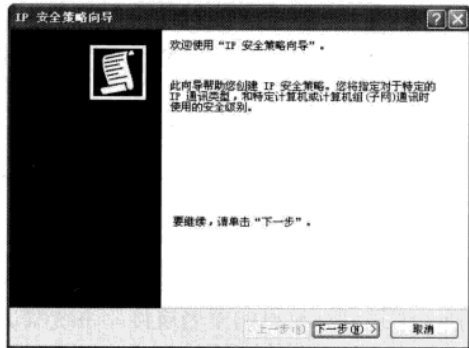
STEP 01 “本地安全设置”窗口

打开“本地安全设置”窗口，在左侧窗格中依次选择“安全设置”|“IP 安全策略”，在本地计算机”选项，如下图所示。



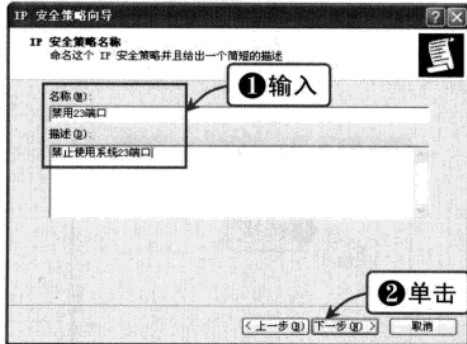
STEP 02 打开“IP 安全策略向导”对话框

在该选项上右击，在弹出的快捷菜单中选择“创建 IP 安全策略”选项，打开“IP 安全策略向导”对话框，如下图所示。



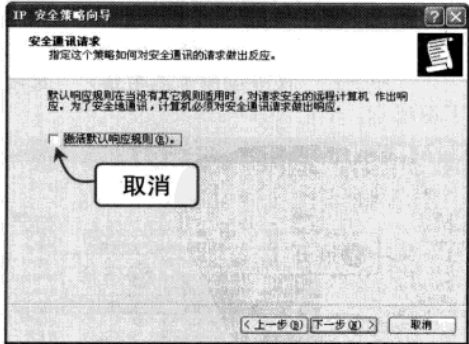
STEP 03 打开“IP 安全策略名称”对话框

单击“下一步”按钮，打开“IP 安全策略名称”对话框，在“名称”文本框中输入所创建的 IP 安全策略的名称，在“描述”文本框中添加对此安全策略的描述信息，单击“下一步”按钮，如下图所示。



STEP 04 打开“安全通讯请求”对话框

打开“安全通讯请求”对话框，取消选择“激活默认响应规则”复选框，如下图所示。



STEP 05 选中“编辑属性”复选框

单击“下一步”按钮，打开“正在完成 IP 安全策略向导”对话框，选中“编辑属性”复选框，单击“完成”按钮，如下图所示。

STEP 06 打开“禁用 23 端口 属性”对话框

在“本地安全策略”窗口中双击刚刚添加的 IP 安全策略选项，打开“禁用 23 端口 属性”对话框，如下图所示。

Chapter 04 设置系统安全策略



STEP 07 打开“新规则 属性”对话框

取消选择“使用‘添加向导’”复选框，然后单击“添加”按钮，打开“新规则 属性”对话框，如下图所示。



STEP 09 打开“筛选器 属性”对话框

单击“添加”按钮，打开“筛选器 属性”对话框，该窗口中包含三个选项卡，即“寻址”、“协议”和“描述”，如下图所示。





STEP 08 打开“IP 筛选器列表”对话框

单击“添加”按钮，打开“IP 筛选器列表”对话框，取消选择“使用‘添加向导’”复选框，如下图所示。



STEP 10 设置源地址和目标地址

在“寻址”选项卡“源地址”下拉列表框中选择“任何 IP 地址”选项，在“目标地址”下拉列表框中选择“我的 IP 地址”选项，如下图所示。

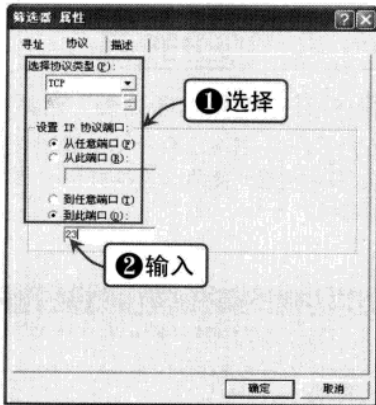


基础知识
与嗅探工具
统漏洞攻防
安全策略
系统与安全
件加密
制攻防
攻防
件攻防
代码攻防
件攻防
毒攻防
安全软件
实用技巧



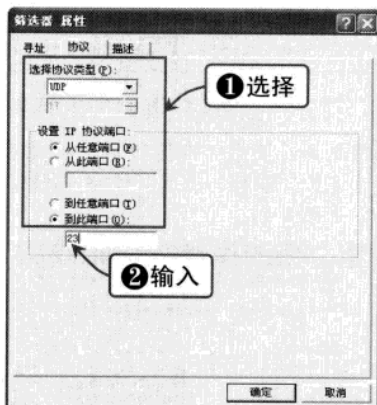
STEP 11 添加 TCP 协议筛选器

选择“协议”选项卡，在“选择协议类型”下拉列表框中选择 TCP 选项，在“设置 IP 协议端口”选项区中选中“从任意端口”和“到此端口”单选按钮，并在“到此端口”下面的文本框中输入 23，如下图所示。单击“确定”按钮，即可添加一个屏蔽 TCP 协议 23 端口的筛选器。



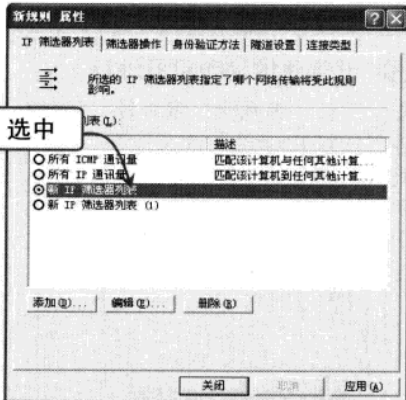
STEP 12 添加 UDP 协议筛选器

重复上述操作，在“筛选器 属性”对话框的“协议”选项卡中设置协议类型为 UDP，在“设置 IP 协议端口”选项区中选中“从任意端口”和“到此端口”单选按钮，并在“到此端口”下面的文本框中输入 23，如下图所示。单击“确定”按钮，即可添加一个屏蔽 UDP 协议 23 端口的筛选器。



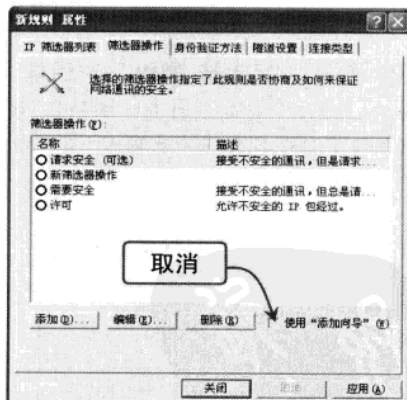
STEP 13 选中“新 IP 筛选器列表”单选按钮

单击“确定”按钮，返回“新规则 属性”对话框，在“IP 筛选器列表”列表中选中“新 IP 筛选器列表”单选按钮，如下图所示。



STEP 14 选择“筛选器操作”选项卡

选择“筛选器操作”选项卡，取消选择“使用‘添加向导’”复选框，如下图所示。



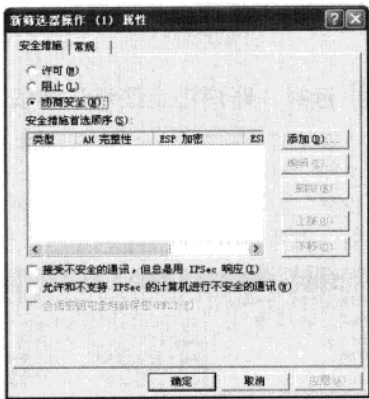
STEP 15 打开“新筛选器操作 属性”对话框

单击“添加”按钮，打开“新筛选器操作 属性”对话框，如下图所示。

STEP 16 增加的“新筛选器操作”选项

在“安全措施”选项卡中选中“阻止”单选按钮，然后单击“确定”按钮，返回“新规则 属性”对话框，在“筛选器操作”列表中将会增加“新筛选器操作”选项，如下图所示。

Chapter 04 设置系统安全策略

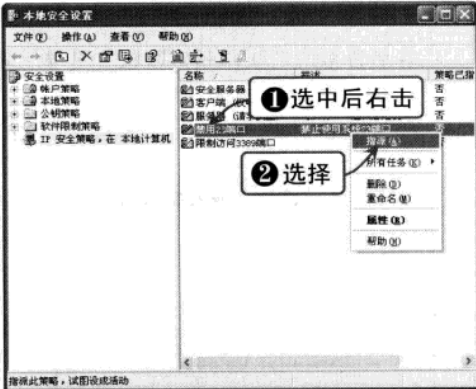
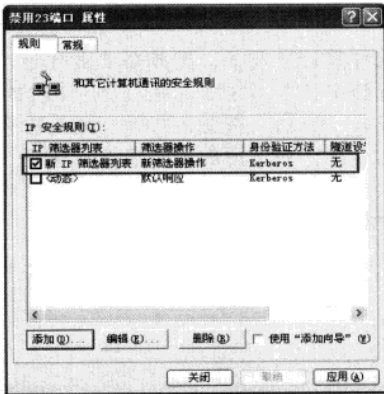


STEP 17 增加“新 IP 筛选器列表”选项

在“筛选器操作”列表选中“新筛选器操作”单选按钮，然后单击“关闭”按钮，返回“禁用 23 端口 属性”对话框，即可看到增加的“新 IP 筛选器列表”选项，且该选项处于被选中状态，如下图所示。

STEP 18 退出 FTP 服务器

依次单击“应用”和“关闭”按钮，即可添加一个禁止 23 端口的 IP 安全策略。重新进入“本地安全设置”窗口，在右侧窗格中选中“禁用 23 端口”选项并右击，从弹出的快捷菜单中选择“指派”选项（如下图所示），即可应用设置。



4.2 设置组策略

组策略指基于组的策略，它以 Windows 中的一个 MMC 管理单元的形式存在，通过它可以帮助系统管理员针对整个计算机或特定用户来设置多种配置。

4.2.1 设置账户锁定策略

账户锁定策略是指当用户在忘记或不知道用户账户和密码的情况下，在输入 X 次（X 代表在组策略中设置好的可以输入的无效输入的次数）无效输入后，Windows 会将登录置为锁定状态。当 Windows 将登录设置为锁定状态后，需要经过一定时间才能被重新启动，这

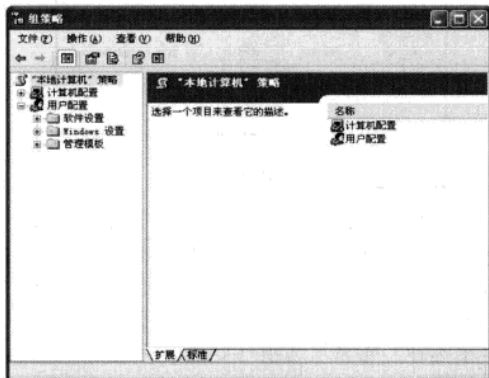
基础知
黑客
常用扫描
与嗅探工具
系统漏洞攻防
Windows 系
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
攻防
聊天软
件攻防
网页恶
意代码
代攻防
电子邮
件攻防
病毒防
C 盘病
使用电
脑安全
软件
黑客攻
防技巧



样黑客便不会轻易地破解出用户账户和密码。
设置账户锁定策略的具体操作方法如下：

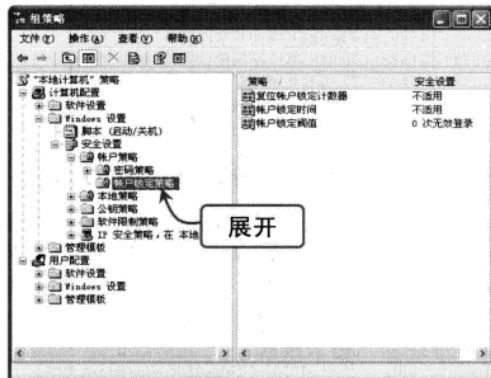
STEP 01 打开“组策略”窗口

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令 gpedit.msc，然后单击“确定”按钮，打开“组策略”窗口，如下图所示。



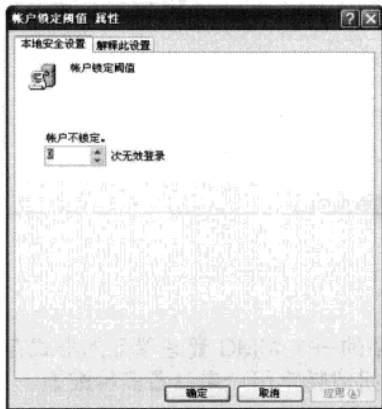
STEP 02 选择“账户锁定策略”选项

在“组策略”窗口中依次展开“本地计算机”策略|“计算机配置”|“Windows 设置”|“安全设置”|“账户策略”|“账户锁定策略”选项，如下图所示。



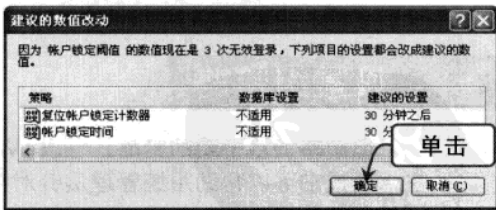
STEP 03 “账户锁定阈值 属性”对话框

在右侧窗格的“账户锁定阈值”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“账户锁定阈值 属性”对话框，如下图所示。



STEP 04 打开“建议的数值改动”对话框

系统默认情况下，无效登录次数为 0，即不设置锁定状态。这里设置无效登录次数为 3，然后单击“应用”按钮，打开“建议的数值改动”对话框，如下图所示。单击“确定”按钮后，其他两个策略选项的数值会自动改为被建议的数值。



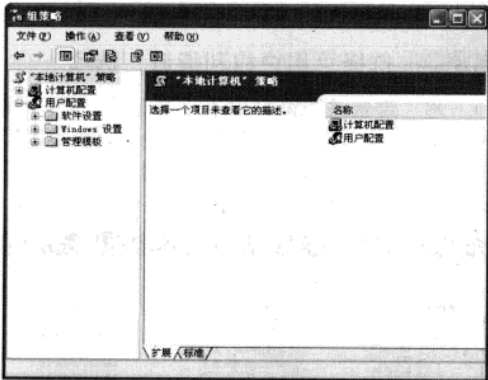
4.2.2 设置密码策略

密码是用户登录操作系统的凭证，只有输入了正确的密码，用户才能正常进入系统。通过设置密码策略，可以加强系统的安全性，在一定程度上能够防止其他用户登录自己的计算机，其具体操作步骤如下：

Chapter 04 设置系统安全策略

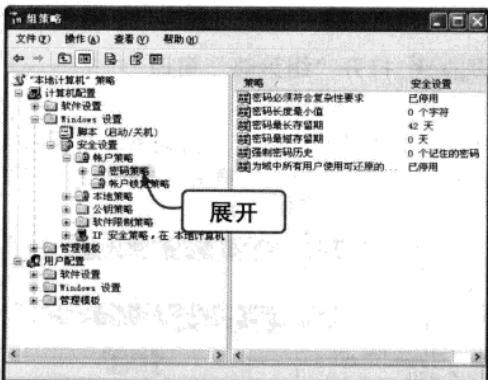
STEP 01 打开“组策略”窗口

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令gpedit.msc，然后单击“确定”按钮，打开“组策略”窗口，如下图所示。



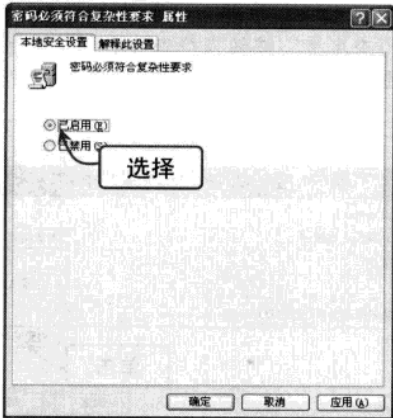
STEP 02 选择“密码策略”选项

在“组策略”窗口中依次展开“本地计算机策略”|“计算机配置”|“Windows 设置”|“安全设置”|“账户策略”|“密码策略”选项，如下图所示。



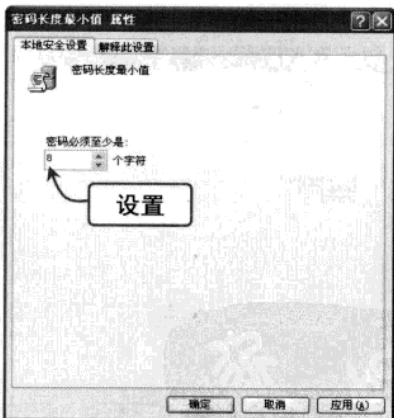
STEP 03 “账户锁定阈值 属性”对话框

在右侧窗格的“密码必须符合复杂性要求”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“密码必须符合复杂性要求 属性”对话框，选中“已启用”单选按钮，如下图所示。



STEP 04 打开“建议的数值改动”对话框

单击“确定”按钮返回“组策略”窗口，在右侧窗格中双击“密码长度最小值”选项，打开“密码长度最小值 属性”对话框，在该对话框中设置用户账户密码包含的最少字符数，如下图所示。



提示



单击“确定”按钮返回，参照上述方法，在“组策略”窗口中可以继续设置其他密码策略。

黑客

常用扫描与嗅探工具

系统安全

设置系统安全策略

系统与文件加密

远程攻击

木马

聊天软件

网页恶意代码

电子邮件攻击

C盘病毒

使用安全软件

黑客攻防技巧

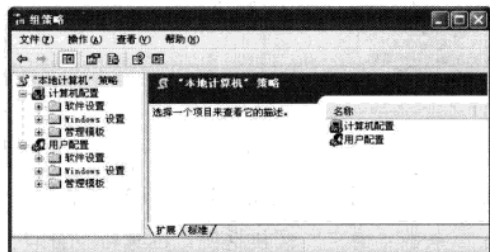


4.2.3 设置用户权限

在与他人共用一台计算机时，为了保护自己的文件安全，可以对各个用户账户设置不同的权限级别。设置用户权限的方法分为两种：一种是通过“创建全局对象”选项中的指派用户权限来设置，另一种是通过“跳过遍历检查”选项中的指派用户权限来设置。这里以通过“创建全局对象”选项设置用户权限为例进行介绍，其具体操作方法如下：

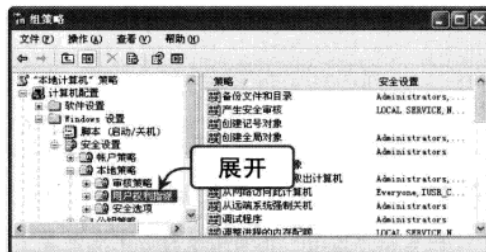
STEP 01 打开“组策略”窗口

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令gpedit.msc，然后单击“确定”按钮，打开“组策略”窗口，如下图所示。



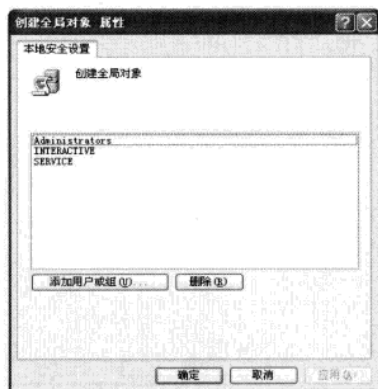
STEP 02 选择“用户权利指派”选项

在“组策略”窗口中依次展开“本地计算机策略”|“计算机配置”|“Windows 设置”|“安全设置”|“本地策略”|“用户权利指派”选项，如下图所示。



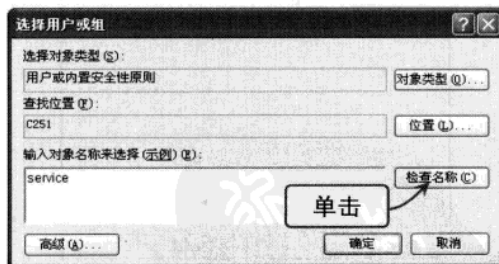
STEP 03 打开“创建全局对象 属性”对话框

在右侧窗格的“创建全局对象”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“创建全局对象 属性”对话框，如下图所示。



STEP 04 打开“建议的数值改动”对话框

单击“添加用户或组”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择（示例）”文本框中输入一个对象名称（可以单击“检查名称”按钮来检查该名称是否存在），如下图所示。



STEP 05 进入高级选项界面

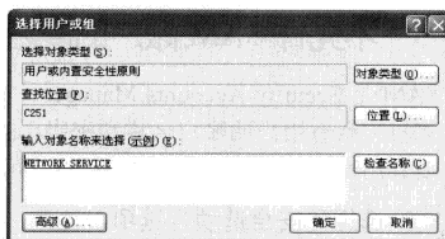
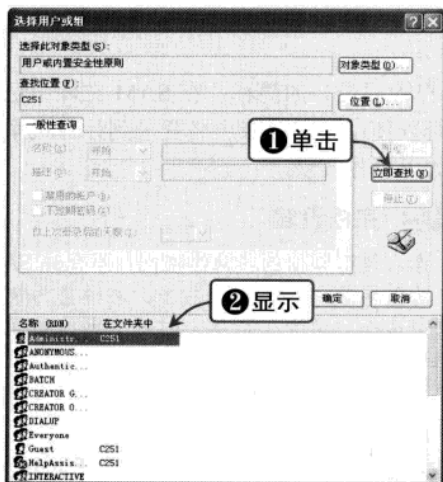
如果不知道要添加的用户或组名称，可以单击“高级”按钮，进入高级选项界面，然后单击“立即查找”按钮，系统将列出当前的用户或组，如下图所示。

STEP 06 添加用户或组

选中要添加的对象，然后单击“确定”按钮返回“选择用户或组”对话框，此时用户可以发现选中的用户或组已经添加到“输入对象名称来选择（示例）”文本框中，单击“确定”按钮，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 04 设置系统安全策略



提示

如果知道用户或组的名称，也可以直接输入。

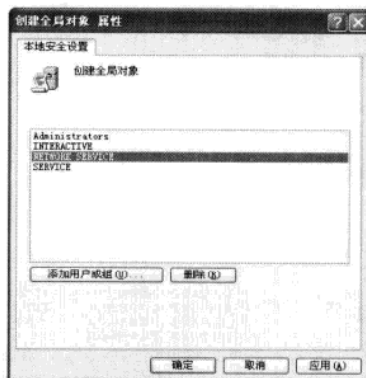
STEP 07 返回“创建全局对象 属性”对话框

返回“创建全局对象 属性”对话框，用户可以发现相应的用户或组的名称被添加到列表中，这样即可将全局权限赋予该特定用户，如右图所示。



提示

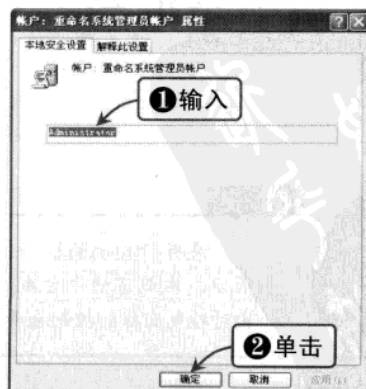
如果不想赋予某账户全局权限，可在上述对话框中将其删除。



4.2.4 更改系统默认的管理员账户

当用户忘记计算机密码时，可以通过系统默认的 Administrator 管理账号登录计算机。这为系统安全带来了一定隐患，用户可以通过更改系统默认的管理员账户来排除此问题，其具体操作步骤如下：

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令“gpedit.msc”，然后单击“确定”按钮，打开“组策略”窗口。在右侧窗格中的“账户：重命名系统管理员账户”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“账户：重命名系统管理员账户 属性”对话框，在其文本框中输入账户名称（如右图所示），然后依次单击“应用”和“确定”按钮即可。



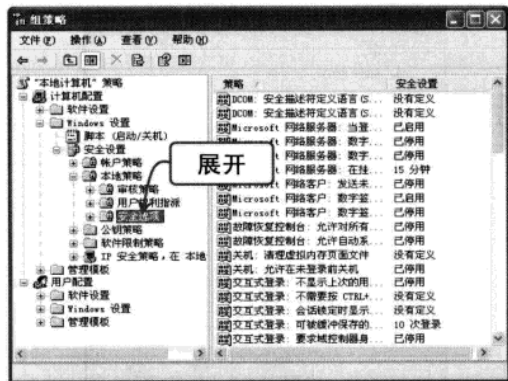


4.2.5 不允许 SAM 账户的匿名枚举

SAM 是 Security Accounts Manager（安全性账户管理员）的简称，在 SAM 文件中记录了计算机中所有用户的账户名称和密码，这样用户可以使用不同的账户名登录到计算机系统中。要禁用 SAM 账户的匿名枚举功能，可以通过如下操作实现：

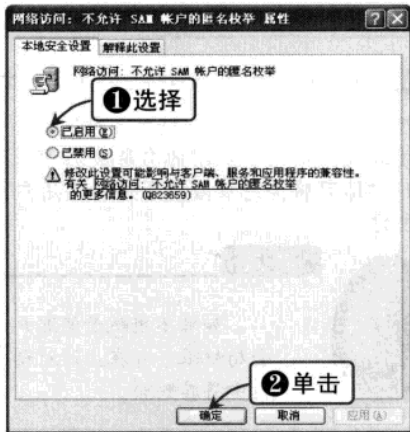
STEP 01 选择“安全选项”选项

打开“组策略”窗口，在左侧窗格中依次展开“‘本地计算机’策略”|“计算机配置”|“Windows 设置”|“安全设置”|“本地策略”|“安全选项”选项，如下图所示。



STEP 02 完成设置

在右侧窗格中的“网络访问：不允许 SAM 账户的匿名枚举”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“网络访问：不允许 SAM 账户的匿名枚举 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“确定”按钮即可。



4.2.6 禁止访问控制面板

通过控制面板可以添加或删除程序、更改用户账号和密码，为了防止其他用户进行上述操作，可以禁止访问控制面板，其具体操作步骤如下：

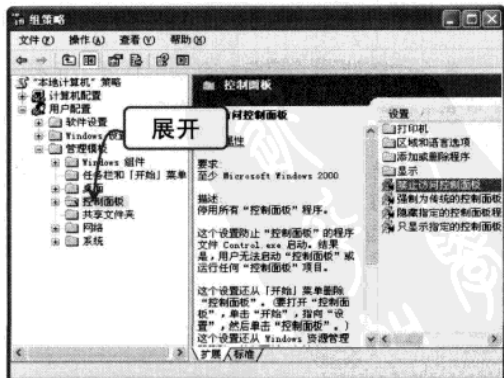
STEP 01 选择“安全选项”选项

打开“组策略”窗口，在左侧窗格中依次展开“‘本地计算机’策略”|“用户配置”|“管理模板”|“控制面板”选项，如右图所示。



提示

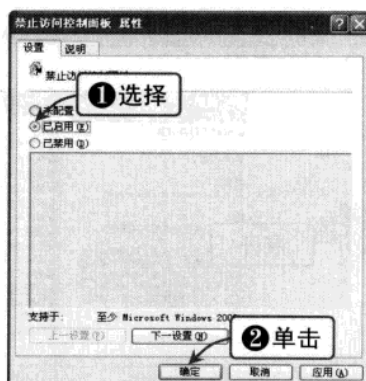
展开“控制面板”选项后，右侧窗格中会显示出对控制面板的控制选项。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

STEP 02 打开“禁止访问控制面板 属性”对话框

在右侧窗格中的“禁止访问控制面板”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“禁止访问控制面板 属性”对话框，选中“已启用”单选按钮（如右图所示），然后单击“确定”按钮即可。

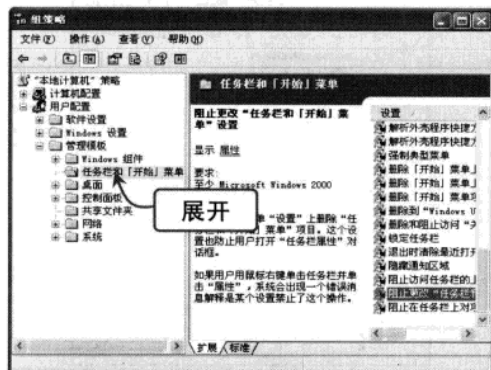


4.2.7 禁止更改“开始”菜单

禁止其他用户更改“开始”菜单的具体操作步骤如下:

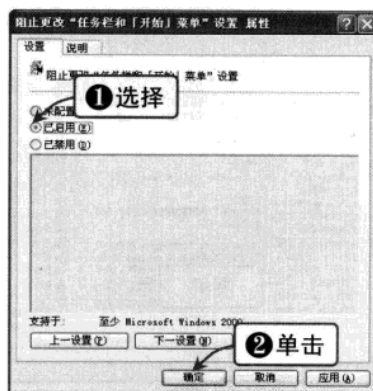
STEP 01 打开“组策略”窗口

打开“组策略”窗口，在左侧窗格中依次展开“‘本地计算机’策略”|“用户配置”|“管理模板”|“任务栏和「开始」菜单”选项，如下图所示。



STEP 02 选中“已启用”单选按钮

在右侧窗格中的“阻止更改‘任务栏和「开始」菜单’设置”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“阻止更改‘任务栏和「开始」菜单’设置 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“确定”按钮即可。



4.2.8 禁止更改桌面设置

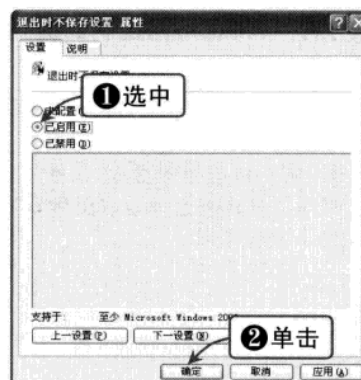
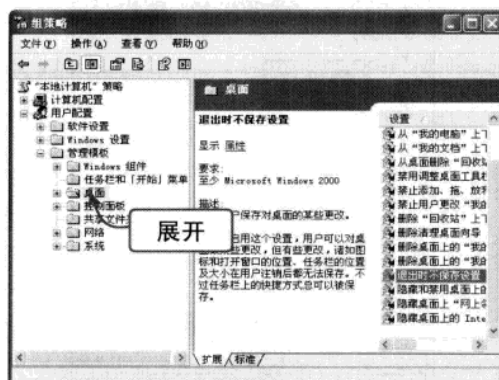
禁止用户更改桌面设置的具体操作步骤如下:

STEP 01 选择“桌面”选项

打开“组策略”窗口，在左侧窗格中依次展开“‘本地计算机’策略”|“用户配置”|“管理模板”|“桌面”选项，如下图所示。

STEP 02 选中“已启用”单选按钮

在右侧窗格中的“退出时不保存设置”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“退出时不保存设置 属性”对话框，选中“已启用”单选按钮（如下图所示），然后单击“确定”按钮即可。

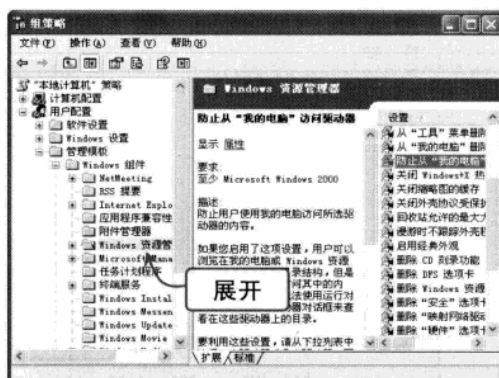


4.2.9 禁止访问指定的磁盘驱动器

禁止访问指定磁盘驱动器的具体设置方法如下：

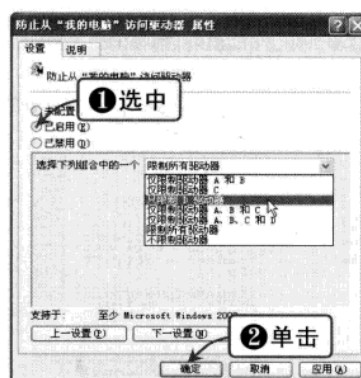
STEP 01 选择“Windows 资源管理器”选项

打开“组策略”窗口，在左侧窗格中依次展开“本地计算机”策略|“用户配置”|“管理模板”|“Windows 组件”|“Windows 资源管理器”选项，如下图所示。



STEP 02 设置防止访问驱动器属性

在右侧窗格中双击“防止从‘我的电脑’访问驱动器”选项，打开“防止从‘我的电脑’访问驱动器 属性”对话框，选中“已启用”单选按钮，并在下面选择一个限制组合（如下图所示），然后单击“确定”按钮即可。



4.2.10 禁用部分应用程序

为了不让他人使用自己的应用程序，用户可以在系统中禁用部分应用程序，其具体操作步骤如下：

STEP 01 选择“软件限制策略”选项

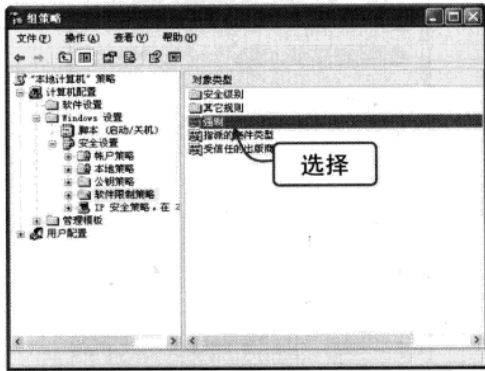
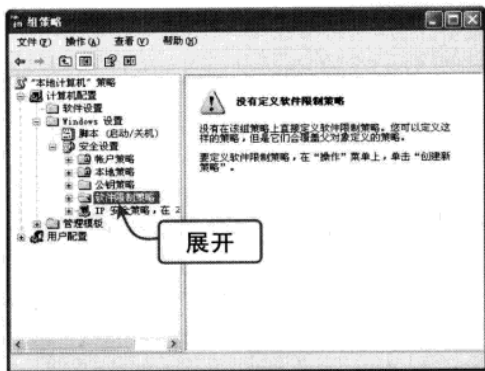
打开“组策略”窗口，在左侧窗格中依次展开“本地计算机”策略|“计算机配置”|“Windows 设置”|“安全设置”|“软件限制策略”选项，如下图所示。

STEP 02 单击“创建新的策略”命令

单击“操作”|“创建新的策略”命令，然后在右侧窗格中选择“强制”选项，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 04 设置系统安全策略

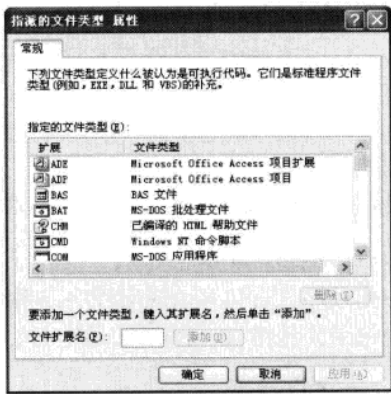
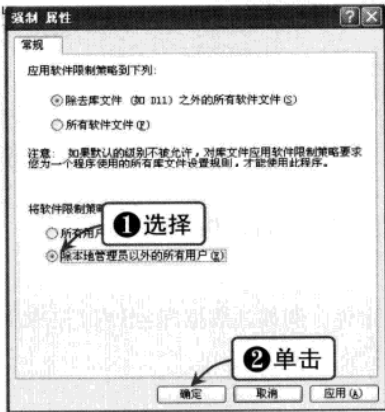


STEP 03 打开“强制 属性”对话框

在“强制”选项上右击，在弹出的快捷菜单中选择“属性”选项，打开“强制 属性”对话框，选中“除本地管理员以外的所有用户”单选按钮，然后依次单击“应用”和“确定”按钮应用设置，如下图所示。

STEP 04 打开“指派的文件类型 属性”对话框

在“组策略”窗口中双击“指派的文件类型”选项，打开“指派的文件类型 属性”对话框，如下图所示。



提示

要在“指派的文件类型 属性”对话框的“指定的文件类型”列表框中添加一种文件类型，可以在“文件扩展名”文本框中输入其扩展名，然后单击“添加”按钮即可。

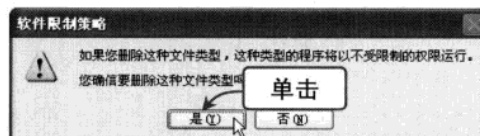
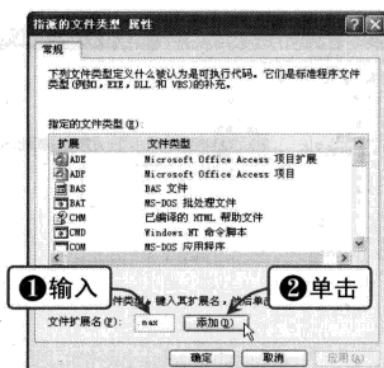
STEP 05 添加文件扩展名

在“指定的文件类型”列表框中显示的是被定义为可执行代码文件的扩展名，可以在“文件扩展名”文本框中输入文件扩展名，然后单击“添加”按钮，如下图所示。

STEP 06 添加用户或组

在“指定的文件类型”列表框中选择某个文件扩展名，然后单击“删除”按钮，打开“软件限制策略”对话框，单击“是”按钮即可删除此文件类型，如下图所示。

基础知识
与嗅探工具
系统漏洞攻防
常用扫描
设置系统
安全策略
系统与安全
件加密
远程控制
木马
聊天软
网页恶
代码攻
件攻防
电子邮
C盘病
使用电
安全软
黑客攻
实用技



4.3 设置计算机管理策略

“计算机管理”是 Windows 管理控制台中的管理工具集，可以用于管理单个的本地或远程计算机，它将几个管理程序合并到控制台树中，并提供对管理属性和工具的快速访问。

4.3.1 事件查看器的使用

Windows 系统的事件查看器是 Windows 2000/XP 中提供的一个系统安全监视工具。在事件查看器中，可以通过使用事件日志，收集有关硬件、软件、系统问题方面的信息，并监视 Windows 系统安全。它不但可以查看系统运行日志文件，而且还可以查看事件类型，使用事件日志来解决系统故障。

使用事件查看器，可以查看并管理应用程序日志、安全性日志和系统日志等。

1. 应用程序日志

应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误，程序开发人员决定监视哪些事件。

2. 安全性日志

安全性日志可以记录诸如有效和无效的登录尝试等事件以及与资源使用有关的事件，例如创建、打开或删除文件。管理器可以指定在安全性日志中记录什么事件，例如，如果您已启用登录审核，登录系统的尝试将记录在安全性日志里。

3. 系统日志

系统日志包含 Windows XP 的系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。Windows XP 预先确定由系统组件记录的事件类型。

查看事件管理器中的日志文件的具体操作步骤如下：

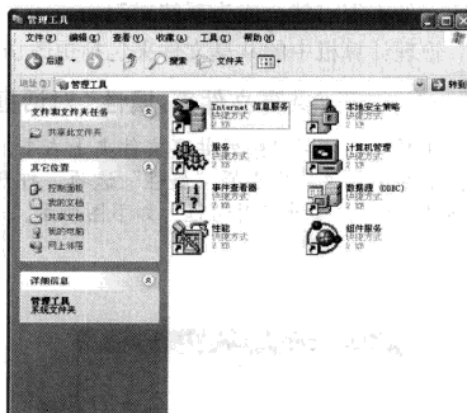
STEP 01 双击“管理工具”图标

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，如下图所示。

STEP 02 双击“事件查看器”图标

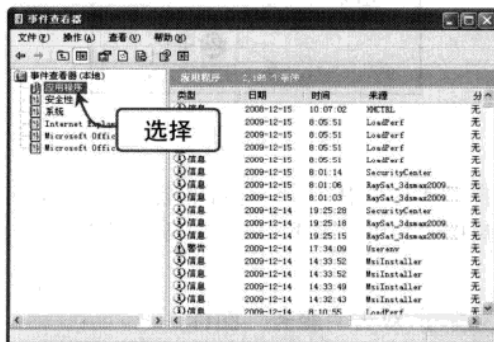
打开“管理工具”窗口，双击“事件查看器”图标，如下图所示。

Chapter 04 设置系统安全策略



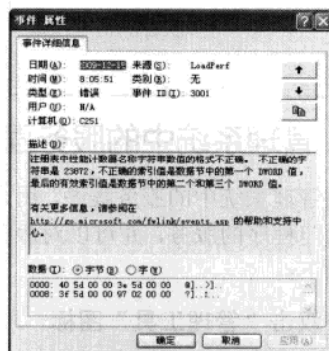
STEP 03 选择“应用程序”选项

打开“事件查看器”窗口，在左侧窗格中选择“事件查看器（本地）”|“应用程序”选项，在右侧窗格中将显示出有关应用程序的所有日志信息，如下图所示。



STEP 04 “事件 属性”对话框

在右侧窗格中，系统使用不同的图标表示不同的日志信息，双击要查看的日志信息，即可打开相应的“事件 属性”对话框，如下图所示。



STEP 05 保存日志文件

在“事件查看器”窗口的左侧窗格中选择“应用程序”选项，在该选项上右击，在弹出的快捷菜单中选择“另存为日志文件”选项，打开“将‘应用程序’另存为”对话框（如右图所示），设置文件名和日志文件的保存路径，然后单击“保存”按钮，即可保存日志。



4.3.2 共享资源的管理

如果用户的计算机处于局域网中，为了工作需要经常要与其他同事共享文件，而这些共

基础知
识

与嗅探
工具

统漏洞
攻防

安全策
略

件加密

制攻防

攻防

件攻防

代码防

件攻防

件攻防

件攻防

件攻防

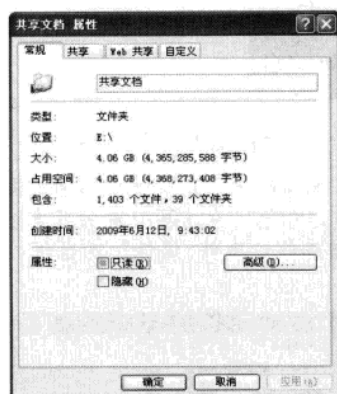


享的文件夹很可能会成为系统漏洞。

管理计算机中的共享文件夹包括更改访问权限、停止共享等，其具体操作方法如下：

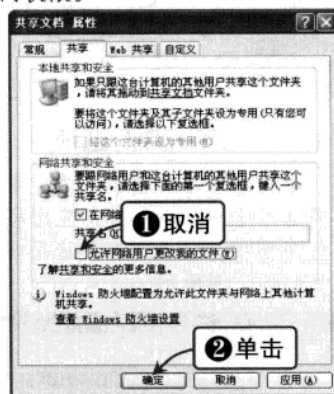
STEP 01 打开“共享文件夹 属性”对话框

在要更改访问权限的共享文件夹上右击，在弹出的快捷菜单中选择“属性”选项，打开“共享文件夹 属性”对话框，如下图所示。



STEP 02 取消选择“允许网络用户更改我的文件”复选框

选择“共享”选项卡，在“网络共享和安全”选项区中取消选择“允许网络用户更改我的文件”复选框（如下图所示），然后依次单击“应用”和“确定”按钮，即可更改共享文件夹的访问权限。



4.3.3 管理系统中的服务程序

通过管理系统中的服务程序，用户可以了解自己计算机中当前运行着哪些服务程序，是否存在后门程序的服务，并可以对服务程序进行启用或禁用。管理系统中服务程序的具体操作步骤如下：

STEP 01 双击“管理工具”图标

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，如下图所示。



STEP 02 双击“服务”图标

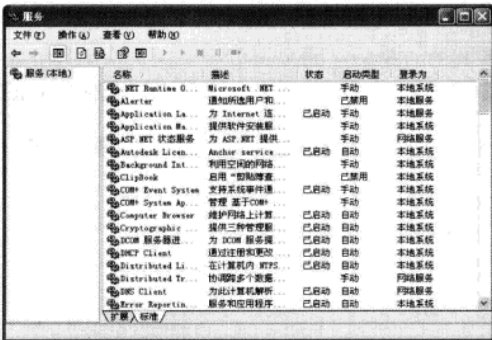
打开“管理工具”窗口，双击“服务”图标，如下图所示。



Chapter 04 设置系统安全策略

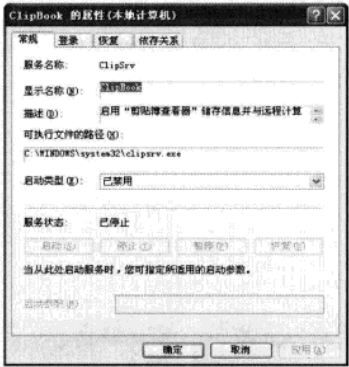
STEP 03 打开“服务”窗口

在打开的“服务”窗口中显示了系统当前所有的后台服务程序，用户可以根据自己的需要来启用或停用相关服务，如下图所示。



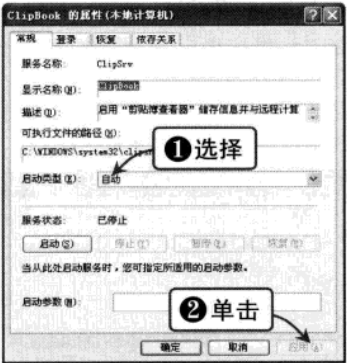
STEP 04 打开“ClipBook 的属性（本地计算机）”对话框

在右侧窗格中双击 ClipBook 选项，打开“ClipBook 的属性（本地计算机）”对话框，如下图所示。



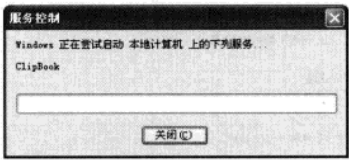
STEP 05 激活“启动”按钮

在“启动类型”下拉列表框中选择“自动”选项，然后单击“应用”按钮，“服务状态”选项区中的“启动”按钮将被激活，如下图所示。



STEP 06 完成程序安装

单击“启动”按钮，弹出“服务控制”对话框，系统开始开启该服务，如下图所示。禁用服务的方法与上述操作相反，用户只需在“启动类型”下拉列表框中选择“已禁用”选项，然后单击“停止”按钮即可。



4.4 设置注册表编辑器安全

在 Windows 操作系统中，注册表编辑区存储着系统软、硬件的有关配置和状态信息，被称为操作系统的核心和灵魂。一旦注册表信息被错误地更改，操作系统很可能运行异常甚至瘫痪。

4.4.1 禁止访问和编辑注册表

为了防止他人随意更改系统的注册表信息，可以禁止访问和编辑注册表，其方法包括以

黑客
常用扫描
与嗅探工具
统漏洞攻防
安全策略
系统与安全
加密
远程控制
攻防
木马
聊天软件
网页恶意
代码攻防
电子邮件
攻击
C 盘病毒
使用电脑
黑客技巧



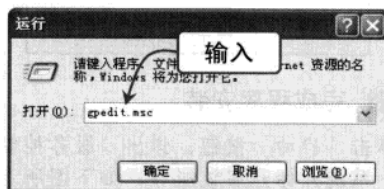
下三种：

Work1 利用“组策略”编辑器

利用“组策略”编辑器禁用注册表编辑器的具体操作方法如下：

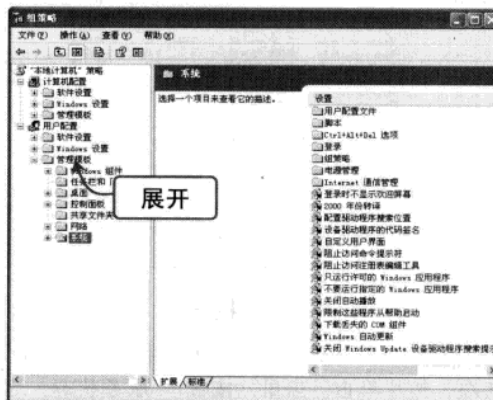
STEP 01 输入 gpedit.msc 命令

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入 gpedit.msc 命令，如下图所示。



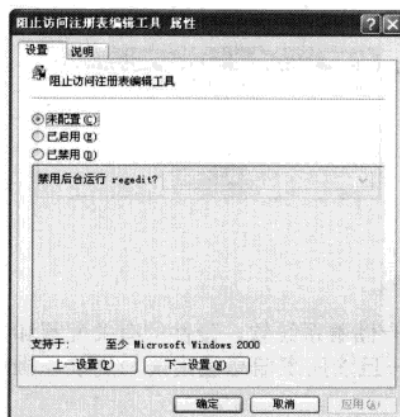
STEP 02 选择“管理模板”选项

打开“组策略”窗口，在左侧窗格中依次展开“本地计算机”策略”|“用户配置”|“管理模板”选项，如下图所示。



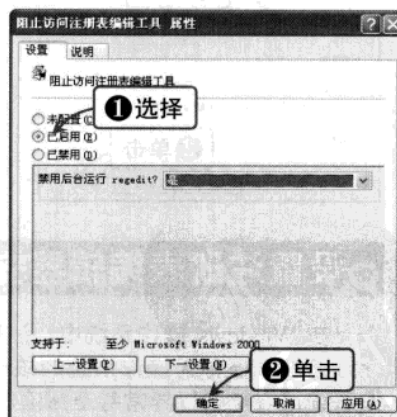
STEP 03 打开“阻止访问注册表编辑工具属性”对话框

在右侧窗格中双击“阻止访问注册表编辑工具”选项，打开“阻止访问注册表编辑工具 属性”对话框，如下图所示。



STEP 04 禁用该服务项

在该对话框中选中“已启用”单选按钮（如下图所示），然后依次单击“应用”和“确定”按钮应用设置，再次打开注册表编辑器时就会提示“注册表编辑已被管理员停用”。



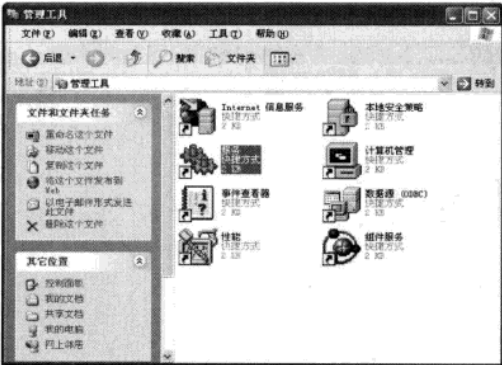
Work2 禁用 Remote Registry 服务

在“服务”窗口中禁用 Remote Registry 服务的具体操作方法如下：

Chapter 04 设置系统安全策略

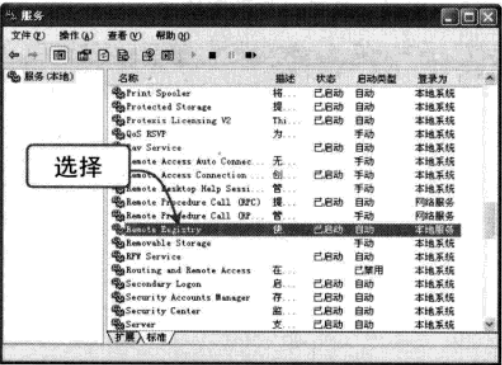
STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，打开“管理工具”窗口，如下图所示。



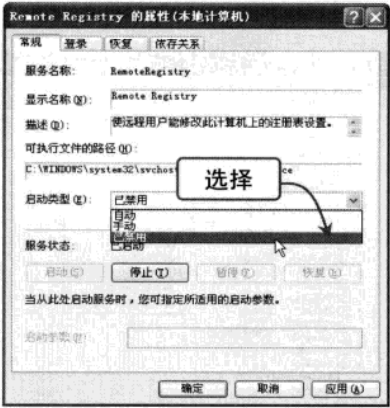
STEP 02 选择 Remote Registry 选项

双击“服务”图标，打开“服务”窗口，在右侧窗格中选择 Remote Registry 选项，如下图所示。



STEP 03 打开“阻止访问注册表编辑工具属性”对话框

双击该选项，打开“Remote Registry 的属性（本地计算机）”对话框，在“启动类型”下拉列表框中选择“已禁用”选项，如下图所示。



STEP 04 禁用该服务项

依次单击“应用”和“停止”按钮（如下图所示），将弹出“服务控制”对话框，然后单击“确定”按钮，即可停止此项服务。



提示

Remote Registry 服务可以使远程用户能修改此计算机上的注册表设置。如果此服务被终止，只有此计算机上的用户才能修改注册表；如果此服务被禁用，任何依赖它的服务将无法启动。

Work3 通过注册表编辑器

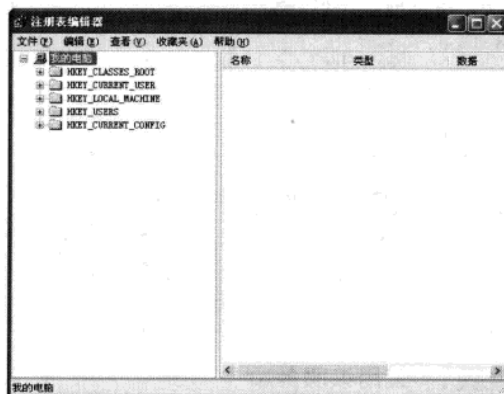
通过注册表编辑器设置禁止访问和编辑注册表的具体操作方法如下：

黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客攻防
实用技巧



STEP 01 打开“注册表编辑器”窗口

单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令 regedit.exe，然后单击“确定”按钮，打开“注册表编辑器”窗口，如下图所示。



STEP 02 展开 Policies 项

在“注册表编辑器”窗口中依次展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies 项，如下图所示。



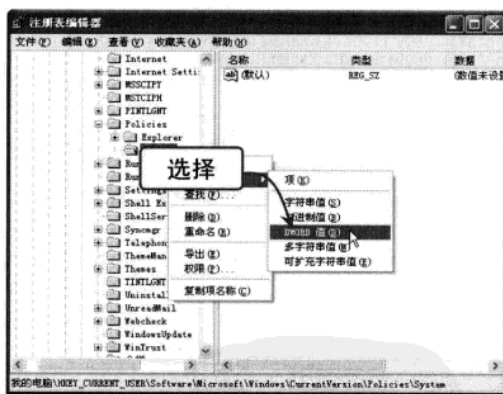
STEP 03 创建 System 主键

在 Policies 键值项上右击，在弹出的快捷菜单中选择“新建”|“项”选项，创建一个名为 System 的主键，如下图所示。



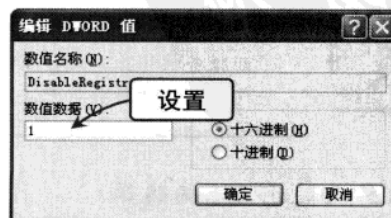
STEP 04 选择“新建”|“DWORD 值”选项

在 System 主键上右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，如下图所示。



STEP 05 激活“启动”按钮

在右侧窗格中创建一个名为 DisableRegistryTools 的 DWORD 值，然后双击该串值，在打开的“编辑 DWORD 值”对话框中设置“数值数据”文本框中的数值为 1，如右图所示。



Chapter 04 设置系统安全策略



提示

在“编辑 DWORD 值”对话框中单击“确定”按钮，然后保存设置并重新启动计算机，用户将不能再对注册表进行编辑。

4.4.2 禁止远程修改注册表

系统默认情况下，Windows 将注册表设置为可以远程调用，而黑客很有可能会利用这个系统漏洞来攻击用户的计算机。要禁用此项功能，可以按照以下步骤进行操作：

STEP 01 展开 winreg 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg 项，如下图所示。



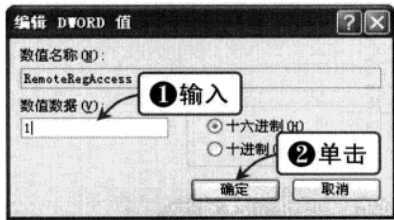
STEP 02 新建子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，新建一个名为 RemoteRegAccess 的子键，如下图所示。



STEP 03 打开“编辑 DWORD 值”对话框

双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1（如右图所示），单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



4.4.3 禁止运行应用程序

通过修改注册表，用户可以禁止运行应用程序，其具体操作步骤如下：

STEP 01 展开 policies 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies 项，如下图所示。

STEP 02 新建 Explorer 主键

在该注册表项上右击，在弹出的快捷菜单中选择“新建”|“项”选项，新建一个名为 Explorer 的主键，如下图所示。

黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



黑客攻防从新手到高手



提示



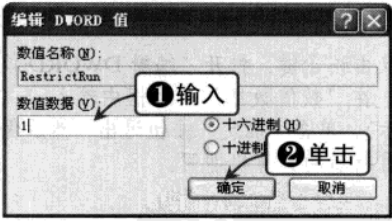
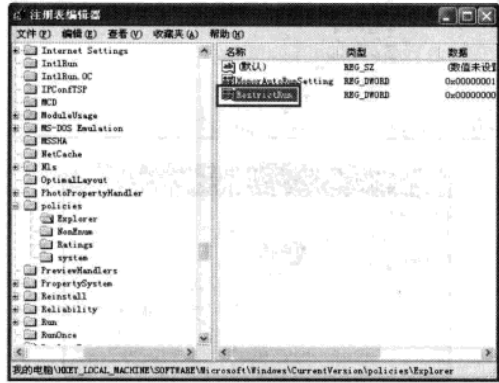
如果该主键已经存在，可以直接选择该主键，进行下面的操作。

STEP 03 新建 RestrictRun 子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，新建一个名为 RestrictRun 的子键，如下图所示。

STEP 04 打开“编辑 DWORD 值”对话框

双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1（如下图所示），单击“确定”按钮完成设置，然后保存设置并重新启动系统即可。



4.4.4 禁止更改系统登录密码

在注册表中禁止更改系统登录密码的具体操作方法如下：

STEP 01 展开 Policies 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies 项，如下图所示。

STEP 02 新建 System 子键

在该选项上右击，在弹出的快捷菜单中选择“新建”|“项”命令，新建一个名为 System 的项，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 04 设置系统安全策略

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

名称 类型 数据

默认值 数值未设置

展开

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

名称 类型 数据

默认值 数值未设置

STEP 03 新建子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，新建一个名为 DisabledChangePassword 的子键，如下图所示。

注册表编辑器

文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)

名称 类型 数据

默认值 数值未设置

DisabledChangePassword

DWORD

0x00000000

STEP 04 禁用该服务项

双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1（如下图所示），单击“确定”按钮完成设置，然后保存设置并重新启动系统即可。

编辑 DWORD 值

数值名称(N): DisabledChangePas

数值数据(V): 1

十六进制(H) 十进制(D)

确定 取消

提示

大家还可以打开“本地安全策略”窗口，在左侧的窗格中展开“安全设置”|“本地策略”|“安全选项”选项，然后在右侧的窗格中启用“域控制器：禁用更改机器账户密码”选项。

4.4.5 隐藏控制面板中的图标

为了不让其他用户随意在本机系统上安装或卸载软件，可以在控制面板中将“添加或删除程序”图标隐藏，其具体操作步骤如下：

STEP 01 展开 don't load 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Control Panel\don't load 项，如下图所示。

STEP 02 新建 appwiz.cpl 子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“字符串值”选项，新建一个名为 appwiz.cpl 的子键，如下图所示。

黑客
基础知识
常用扫描
与嗅探工具
系统漏洞攻防
Windows 系
统设置
安全策略
系统与文
件加密
远程控制
木马
聊天软
件攻防
网页恶意
代码攻防
电子邮箱
C 盘病
使用电脑
黑客攻防
实用技巧

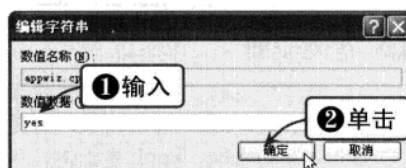
103

溜客安全网 WwW.176Ku.CoM



STEP 03 打开“编辑字符串”对话框

双击该子键，打开“编辑字符串”对话框，在“数值数据”文本框中输入 yes（如右图所示），单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



4.4.6 禁止 IE 浏览器查看本地磁盘

系统默认情况下，用户可以在 IE 浏览器的地址栏中通过输入本地磁盘路径来查看本地磁盘，我们可以通过修改注册表将此功能禁用，其具体操作步骤如下：

STEP 01 展开 Explorer 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 项，如下图所示。



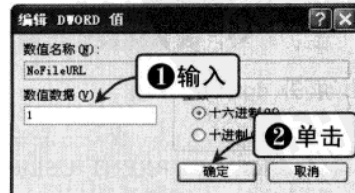
STEP 02 新建 NoFileURL 子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，新建一个名为 NoFileURL 的子键，如下图所示。



STEP 03 打开“编辑 DWORD 值”对话框

双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1（如右图所示），单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



Chapter 04 设置系统安全策略

4.4.7 关闭默认共享

系统默认情况下，Windows XP 常常会将 C\$、D\$ 和 admin\$ 等类型设置为共享，用户可以注册表编辑区中进行相应设置，将这些共享关闭，其具体操作步骤如下：

STEP 01 展开 Lsa 项

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 项，如下图所示。



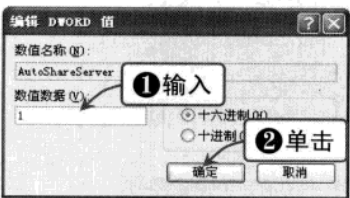
STEP 02 新建 AutoShareServer 子键

在右侧窗格中右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，新建一个名为 AutoShareServer 的子键，如下图所示。



STEP 03 打开“编辑 DWORD 值”对话框

双击该子键，打开“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 1（如右图所示），单击“确定”按钮退出，然后保存设置并重新启动计算机即可。



基础知识

常用扫描工具

系统漏洞扫描

设置系统安全策略

系统与文件加密

远程控制

木马

聊天软件

网页恶意代码

电子邮件

C 盘病毒

使用电脑安全软件

黑客攻防实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter

05

系统与文件加密

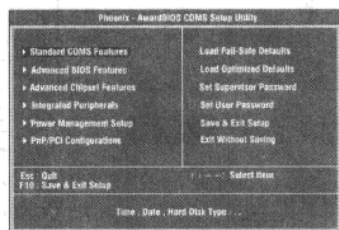
为了保障系统与文件的安全，我们需要对它们进行层层加密，通过一个个严密的“安全锁”将其保护起来，才能让那些网络黑客无机可乘。本章将详细介绍为操作系统加密、为文件加密、使用加密软件加密以及破解管理员账户等知识，读者应该熟练掌握。

本章建议学习时间：

本章建议学习时间为 50 分钟，其中分配 25 分钟学习系统与文件加密的相关知识，25 分钟观看教学视频并进行练习。

学完本章后您可以：

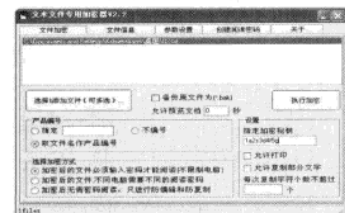
- 设置 CMOS 开机密码
- 设置系统启动密码
- 为 Word 文档加密
- 为电子邮件加密
- 使用加密软件进行加密
- 破解系统管理员账户



BIOS 设置程序界面



“用户账户”窗口



指定加密密钥

重要知识点视频索引



5.1 为操作系统加密

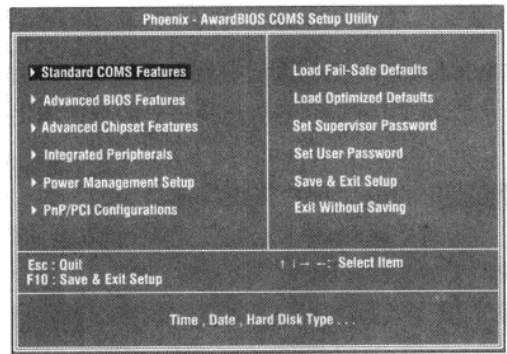
要想不被黑客轻而易举地闯进自己的操作系统，为操作系统加密是最基本的操作。不加密的系统就像自己的家开了一个任人进出的后门，其他用户都可以随意打开用户的系统，查看用户电脑上的私密文件。

5.1.1 设置 CMOS 开机密码

CMOS 在电脑的硬件设备中有着特殊的作用，它保存着电脑启动的基本信息。用户可以在 CMOS 中设置系统开机密码，当系统开机后只有输入正确的密码，才会启动操作系统。设置 CMOS 开机密码的具体操作方法如下：

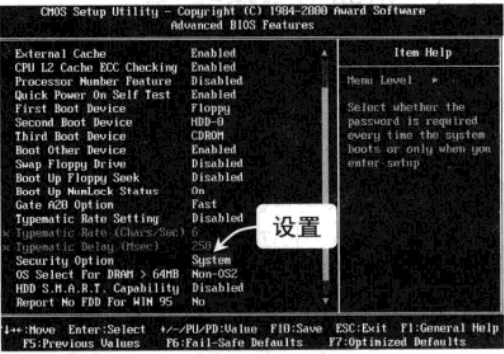
STEP 01 BIOS 设置程序界面

按下主机上的开机键，在出现开机画面时按【Delete】键（部分电脑是【F2】键），进入 BIOS 设置程序界面，如下图所示。



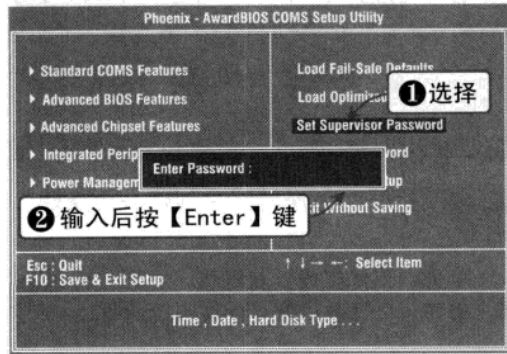
STEP 02 将 Security Option 设为 System

选择 Advanced BIOS Features 选项，进入高级 BIOS 设置界面，然后将 Security Option 项设置为 System，如下图所示。



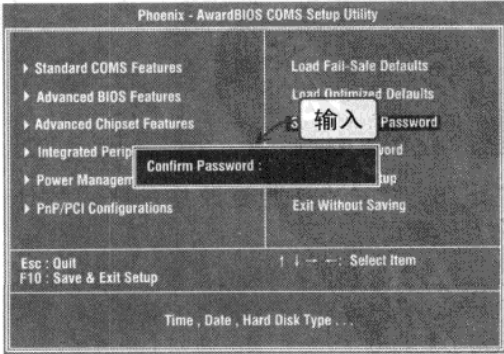
STEP 03 BIOS 密码设置提示框

在 BIOS 设置程序主界面中选择 Set Supervisor Password 选项，在 BIOS 密码设置提示框中输入密码，然后按【Enter】键确认。



STEP 04 再次输入密码确认

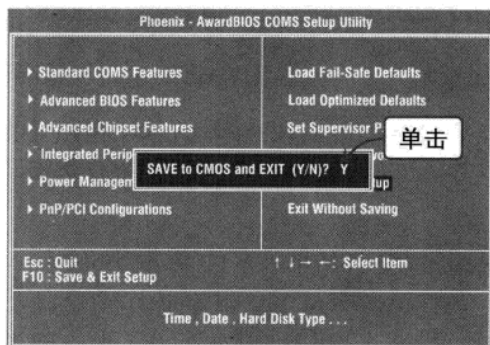
再次输入密码确认，即可完成开机密码设置，如下图所示。





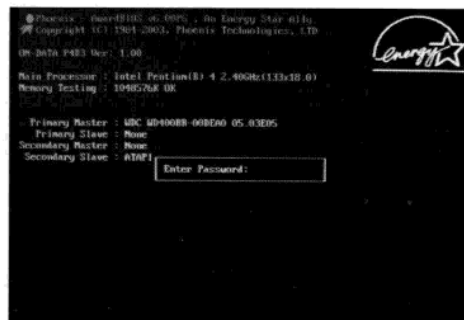
STEP 05 是否保存并退出提示框

在 BIOS 设置主界面中选择 Save & Exit Setup 选项，然后按【Enter】键，就会弹出是否保存并退出的提示框，按【Y】键确认，即可保存设置并退出 BIOS 设置程序，如下图所示。



STEP 06 开始显示界面

重新启动电脑后，在开始显示界面就会出现提示，让用户输入开机密码，如下图所示。



5.1.2 设置系统启动密码

为了不让他人随意使用自己的电脑，可以在 Windows XP 操作系统中为自己的账户添加系统启动密码，这样不知道此密码的人就没办法登录系统了。设置系统启动密码的具体操作步骤如下：

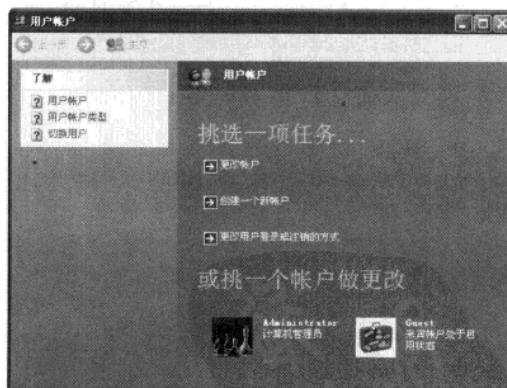
STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，如下图所示。



STEP 02 打开“用户账户”窗口

双击“用户账户”图标，打开“用户账户”窗口，如下图所示。



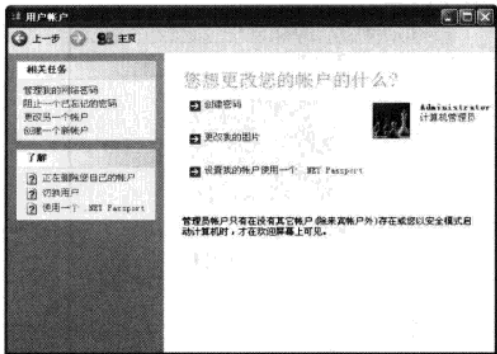
STEP 03 打开“您想更改您的账户的什么？”窗口

单击要设置登录密码的账户，在此以计算机管理员账户为例，单击该账户打开“您想更改您的账户的什么？”窗口，如下图所示。

STEP 04 打开“为您的账户创建一个密码”窗口

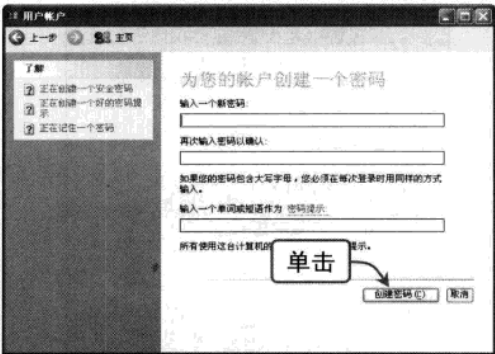
单击“创建密码”超链接，打开“为您的账户创建一个密码”窗口，如下图所示。

Chapter 05 系统与文件加密



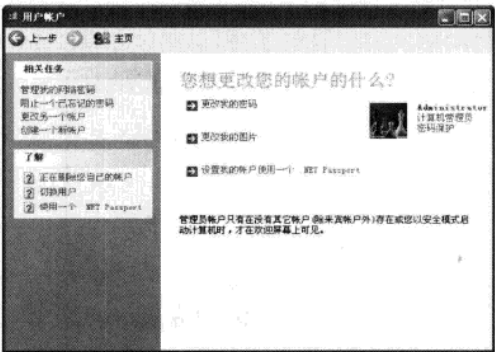
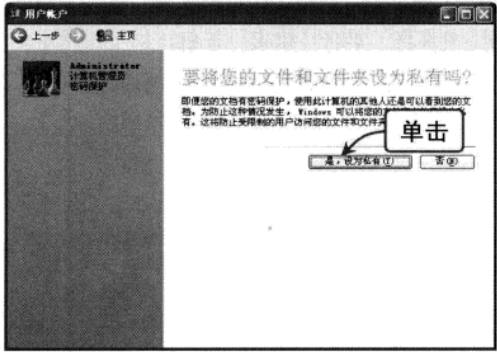
STEP 05 打开“要将您的文件和文件夹设为私有吗？”窗口

在相应的文本框中输入要设置的密码，然后单击“创建密码”按钮，打开“要将您的文件和文件夹设为私有吗？”窗口，单击“是，设为私有”按钮，如下图所示。



STEP 06 开始显示界面

返回“您想要更改您的账户的什么？”窗口（如下图所示），即可完成设置系统启动密码操作。



5.1.3 设置屏幕保护密码

当用户有事需要暂时离开电脑一会儿时，为了方便当然不想频繁开关电脑，但又担心自己不在的时候其他人用自己的电脑，这时可以启用屏幕保护功能，并为屏幕保护程序设置密码，这样就可以保障系统安全了。设置屏幕保护密码的具体操作步骤如下：

STEP 01 打开“显示 属性”对话框

在桌面上的空白位置右击，在弹出的快捷菜单中选择“属性”选项，弹出“显示 属性”对话框，如下图所示。

STEP 02 选择“屏幕保护程序”选项卡

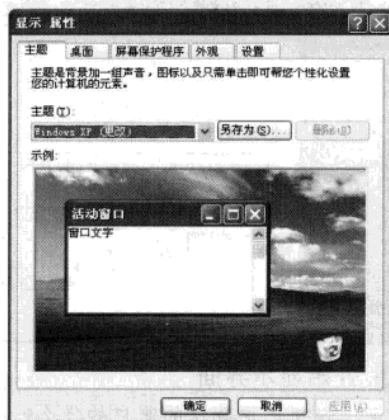
选择“屏幕保护程序”选项卡，在下面的下拉列表框中选择一种屏幕保护程序，并选中“在恢复时使用密码保护”复选框，如下图所示。



提示

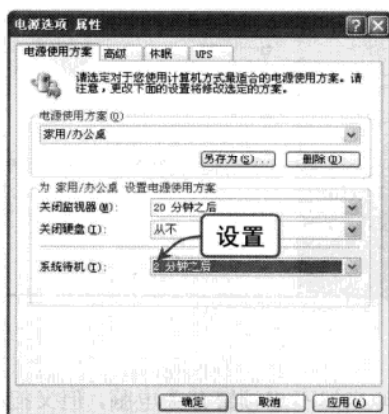
在“屏幕保护程序”选项卡中，用户可以根据自己的实际情况将等待时间设置得短一些，以便自己离开时屏幕保护程序及时开启。

- 基础入门
- 黑客入门
- 常用扫描工具
- 系统漏洞攻防
- 安全策略
- 系统与安全
- 文件加密
- 远程控制
- 木马攻击
- 聊天软件
- 网页恶意代码
- 代码攻防
- 电子邮
- 病毒攻
- 使用电
- 黑客攻



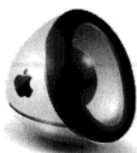
STEP 03 打开“电源选项 属性”对话框

单击“监视器的电源”选项区中的“电源”按钮，弹出“电源选项 属性”对话框，在“系统待机”下拉列表框中设置待机时间，如下图所示。



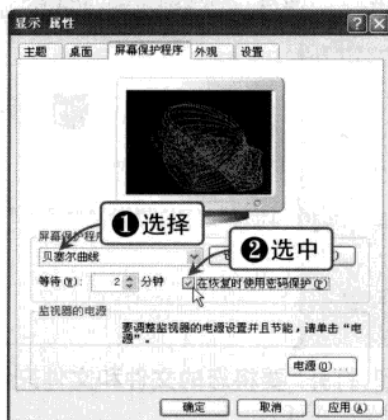
STEP 05 打开“要将您的文件和文件夹设为私有吗？”窗口

此时，即可完成屏幕保护密码设置。当电脑从屏幕保护程序状态下恢复时，就会要求用户输入密码，如右图所示。



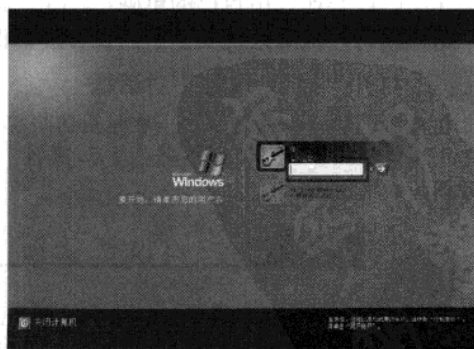
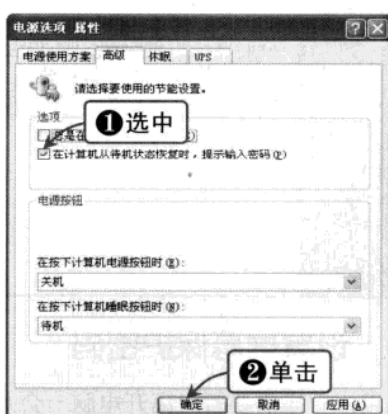
提示

进入屏幕保护程序状态后，系统不会关闭，用户返回后输入密码即可恢复。



STEP 04 选中“在计算机从待机状态恢复时，提示输入密码”复选框

选择“高级”选项卡，在“选项”选项区中选中“在计算机从待机状态恢复时，提示输入密码”复选框，单击“确定”按钮，如下图所示。



5.2 为文件加密

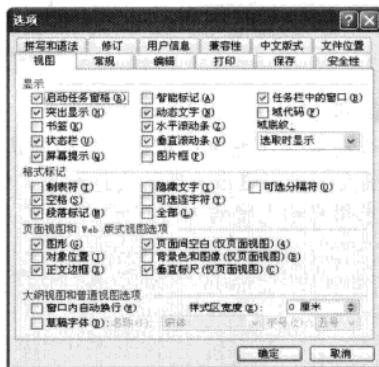
为了保障系统中各种文件的安全，可以对不同的文件进行加密，当然其方式也各不相同，下面将详细讲解文件加密的方法。

5.2.1 为 Word 文档加密

Word 是最常用的文字处理软件，为自己的 Word 文档加密的具体操作步骤如下：

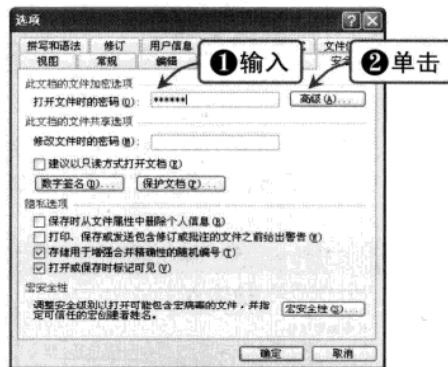
STEP 01 打开“选项”对话框

启动 Word 2003，单击“工具”|“选项”命令，弹出“选项”对话框，如下图所示。



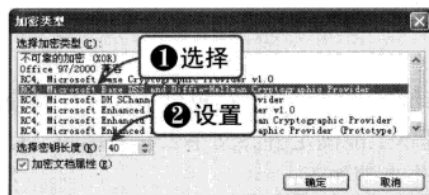
STEP 02 “安全性”选项卡

选择“安全性”选项卡，在“打开文件时的密码”文本框中输入密码，单击“高级”按钮，如下图所示。



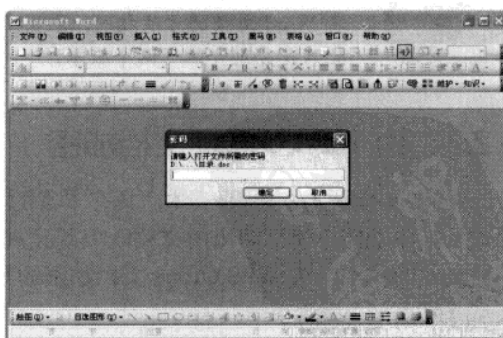
STEP 03 “加密类型”对话框

弹出“加密类型”对话框，在“选择加密类型”列表框中选择密码的加密方式，然后在“选择密钥长度”数值框中设置密钥长度，如下图所示。



STEP 04 加密 Word 文档后的效果

依次单击“确定”按钮应用设置，当下次打开此文档时，系统将要求用户输入密码方可打开，如下图所示。



5.2.2 为 Excel 表格加密

Excel 是最常用的表格处理软件，为了保证表格中的数据安全，同样可以对其进行加密，

黑客

常用扫描
与嗅探工具

系统漏洞攻防

设置系统
安全策略

系统与文
件加密

远程控制
木马

聊天软
件攻防

网页恶意
代码攻防

电子邮件
件攻防

病毒防
安全软件

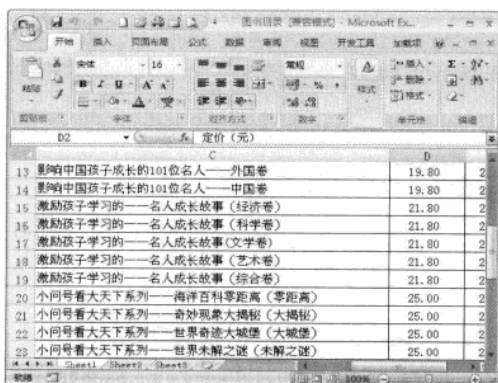
使用电脑
黑客技巧



在此以 Excel 2007 为例进行介绍，其具体操作步骤如下：

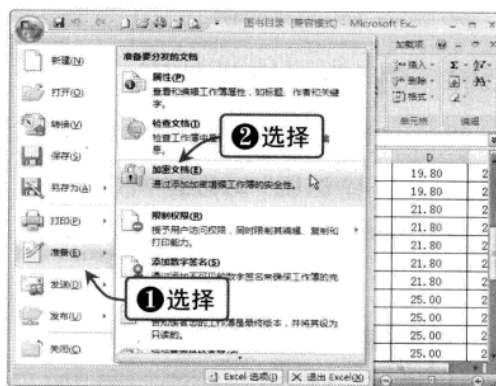
STEP 01 打开一个 Excel 文档

启动 Excel 2007，然后打开一个 Excel 文档，如下图所示。



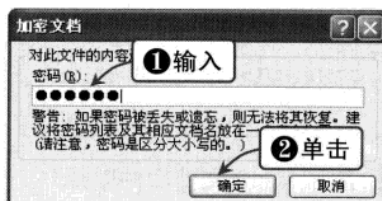
STEP 02 选择“加密文档”选项

单击 Office 按钮，在弹出的下拉菜单中选择“准备”|“加密文档”选项，如下图所示。



STEP 03 打开“加密类型”对话框

在弹出的“加密文档”对话框的“密码”文本框中输入密码，并单击“确定”按钮，如下图所示。



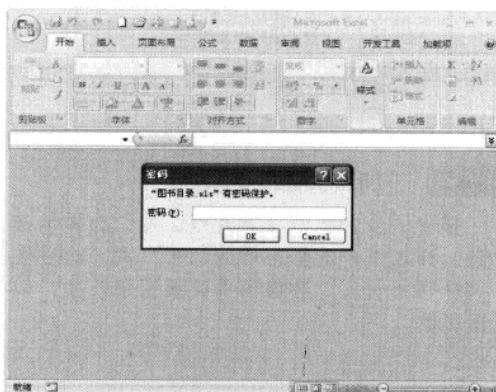
提示



其实加密 Excel 文档与加密 Word 文档的方法相同，在此只是分别介绍了两个版本。

STEP 04 加密 Excel 文档后的效果

在弹出的对话框中重新输入密码确认，并单击“确定”按钮退出。当下次打开此文档时，系统要求用户输入密码方可打开，如下图所示。



5.2.3 为 WPS Office 文档加密

WPS 集编辑与打印于一体，具有丰富的全屏编辑功能，而且还提供了各种控制输出格式及打印功能，使打印出的文稿既美观又规范，基本上能满足各界文字工作者编辑、打印各种文件的需求。为 WPS Office 文档加密的具体操作步骤如下：

STEP 01 打开文件

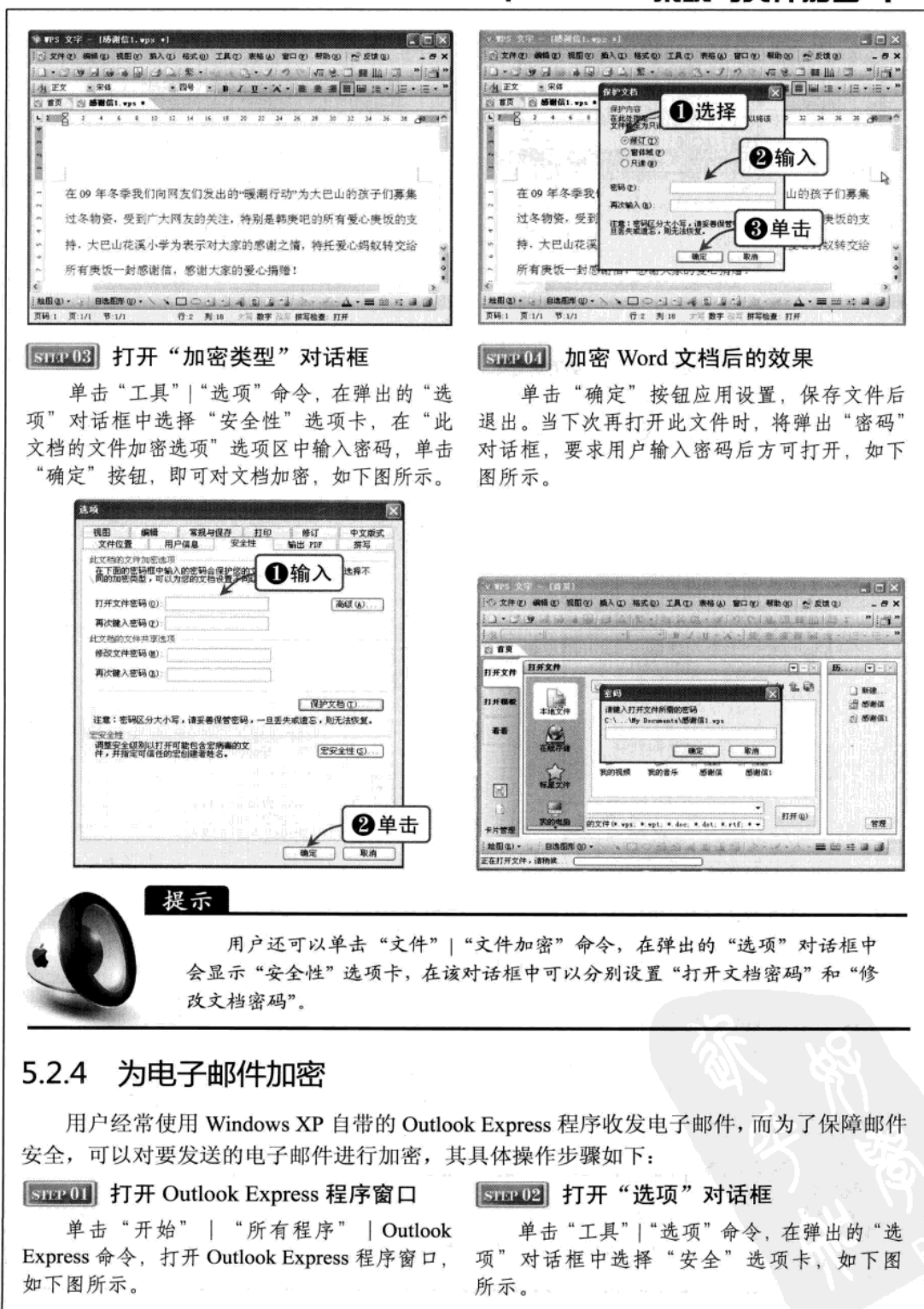
启动 WPS 文字处理程序，单击“文件”|“打开”命令，打开一个 WPS 文字文件，如下图所示。

STEP 02 “保护文档”对话框

单击“工具”|“保护文档”命令，弹出“保护文档”对话框，选中要保护的内容，然后在下方的文本框中输入密码，单击“确定”按钮，即可保护所选中的内容，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 05 系统与文件加密



黑客
基础知识

常用指南
与勘探工具

Windows XP 漏洞攻防防

安全策略

系统与安全
件加密

攻防 木马

天 防
大 國

攻防

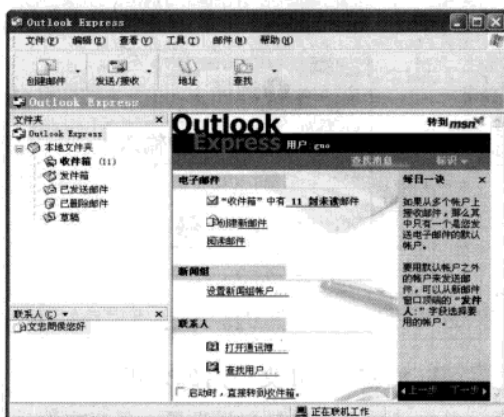
子郵
攻防

攻防 盤病

用电脑
主软件

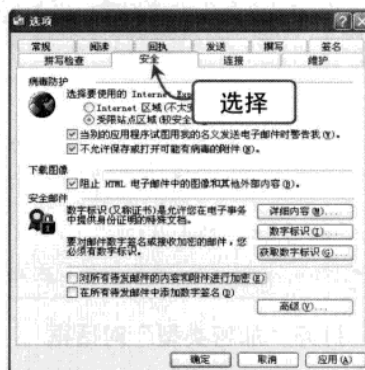
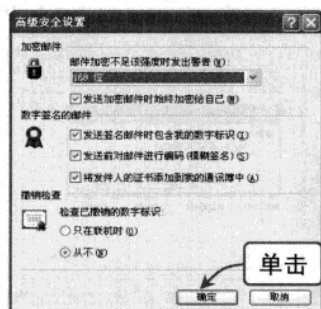
黑客攻防实用技巧

13



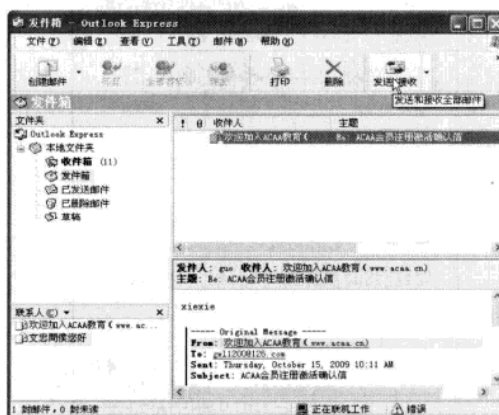
STEP 03 打开“高级安全设置”对话框

在“安全邮件”选项区中选中“对所有待发邮件的内容和附件进行加密”复选框，然后单击“高级”按钮，弹出“高级安全设置”对话框，如下图所示。依次单击“确定”按钮应用设置，保存文件后退出。



STEP 04 加密 Word 文档后的效果

当下次发送邮件及其附件时，系统会自动对它们进行加密。



5.2.5 为压缩文件加密

为了保障文件安全，还可以对压缩文件包进行加密，其具体操作步骤如下：

STEP 01 打开 WinRAR 程序

单击“开始”|“所有程序”|WinRAR|WinRAR 命令，打开 WinRAR 程序，如下图所示。

STEP 02 “压缩文件名和参数”对话框

在文件列表中选中要压缩的文件，单击“添加”按钮，在弹出的“压缩文件名和参数”对话框中选择“高级”选项卡，单击“设置密码”按钮，如下图所示。

提示

压缩文件的格式是多种多样的，用户在“高级”选项卡中可以对“NTFS 选项”、“恢复记录”、“分卷”和“系统”四个选项区中的选项进行设置。

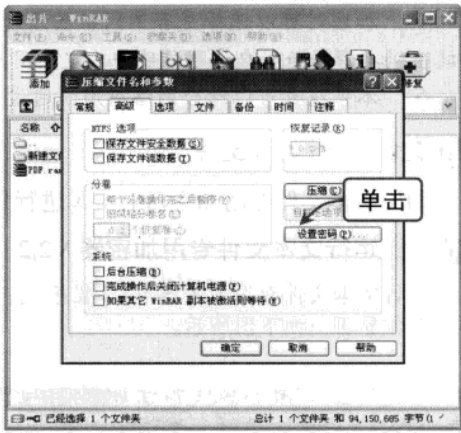
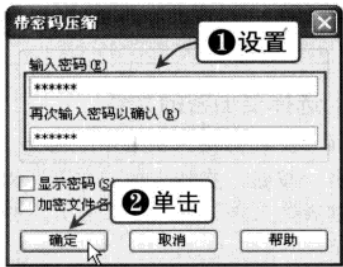
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 05 系统与文件加密



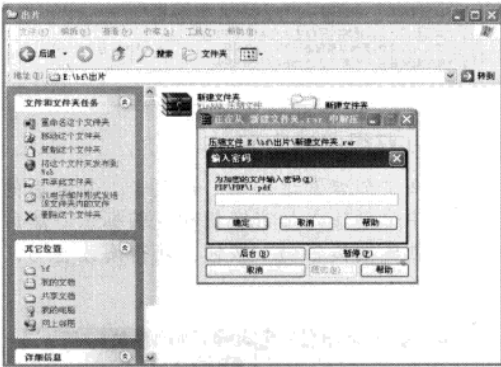
STEP 03 打开“带密码压缩”对话框

在弹出的“带密码压缩”对话框中设置压缩密码，如下图所示。



STEP 04 输入解压缩密码

依次单击“确定”按钮压缩文件，当下次解压缩文件时，系统会自动提示用户输入解压缩密码，如下图所示。



5.3 使用加密软件加密

除了上述方法外，用户还可以利用专门的加密软件对文本、文件和文件夹、程序等进行加密。

5.3.1 文本文件专用加密器

使用文本文件专用加密器可以应用于各种文本文件的保护，如源代码、电子书、资料等，其主要具有以下特点：

- ❖ 可以控制是否允许用户打印文档。
- ❖ 可以控制是否允许客户复制文字，并可以精确控制允许复制的字符数。
- ❖ 可以指定产品编号，以便用户管理多个文件，以免混乱。
- ❖ 可以设置提示语，以便告知用户通过何种途径与用户联系获得阅读密码。
- ❖ 可以定制多个文件共享一个播放授权，同台机器只需要输入一次播放密码。



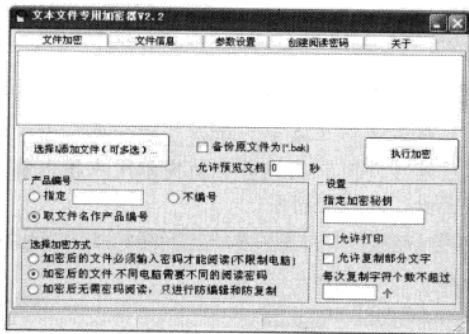
- ❖ 加密时可以选择是否不同机器阅读需要不同的阅读密码，可以为不同用户设置不同的阅读密码，密码与用户的电脑硬件绑定，用户无法传播自己的文件。
- ❖ 本系统也可以结合网络应用，通过网络向客户发放阅读密码、会员验证等方式。

Work1 加密文本文件

利用文本文件专用加密器对文本进行加密的具体操作步骤如下：

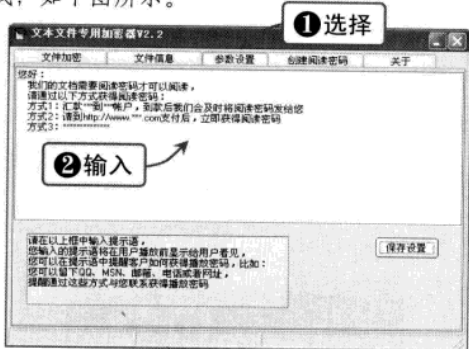
STEP 01 运行文本文件专用加密器 V2.2

运行文本文件专用加密器 V2.2 程序，打开其主工作界面，如下图所示。



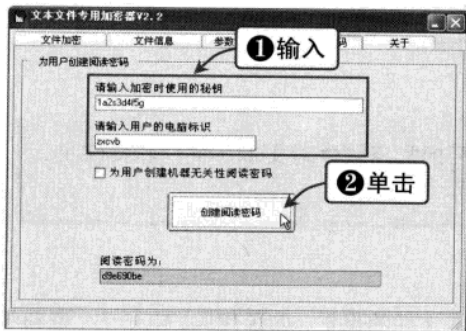
STEP 02 “参数设置”选项卡

选择“参数设置”选项卡，在下面的文本框中输入提示信息，为客户指定获取密码的方式，如下图所示。



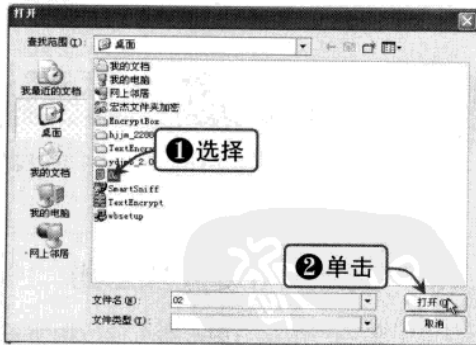
STEP 03 获得阅读密码

选择“创建阅读密码”选项卡，在下面的文本框中分别输入加密密钥和电脑标识，然后单击“创建阅读密码”按钮，获得阅读密码，如下图所示。



STEP 04 选择要加密的文件

选择“文件加密”选项卡，单击“选择&添加文件”按钮，在弹出的“打开”对话框中选择要加密的文件，并单击“打开”按钮，如下图所示。



STEP 05 指定加密密钥

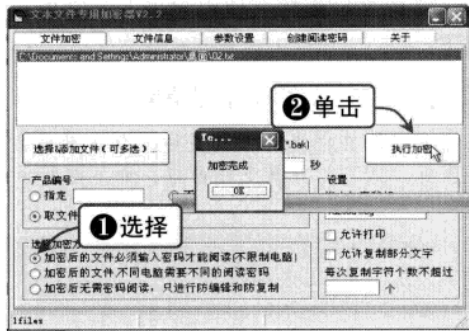
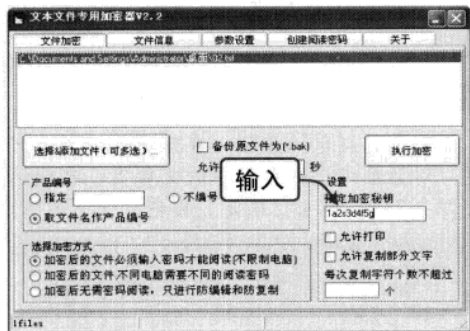
返回主窗口后可以看到刚刚添加的文件，在“设置”选项区的“指定加密密钥”文本框中输入密钥，如下图所示。

STEP 06 完成程序安装

在“选择加密方式”选项区中设置文本加密方式，在此选中“加密后的文件必须输入密码才能阅读（不限制电脑）”单选按钮，如下图所示。单击“执行加密”按钮，即可对文本进行加密。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 05 系统与文件加密



提示

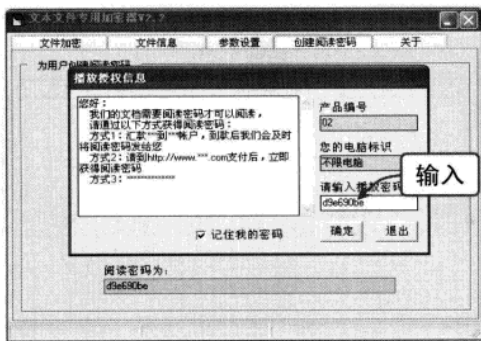
在“选择加密方式”选项区中，可以根据自己的实际情况将加密方式设置为不同的电脑需要不同的阅读密码，或者文件可读，但编辑和复制操作需要密码。

Work2 阅读文本文件

将文本文件加密后，可以利用以下方法阅读此文件：

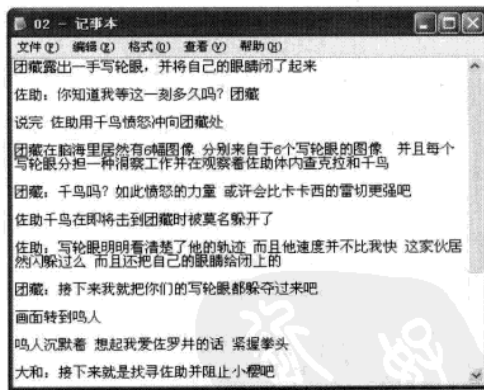
STEP 01 运行 Nmap 扫描程序

在桌面上双击刚刚加密过的文本文件的图标，将弹出提示信息框，单击 OK 按钮，在“播放授权信息”对话框中根据加密器中创建的密码，输入阅读密码，如下图所示。



STEP 02 阅读文本文件

单击“确定”按钮，即可打开此文本文档，阅读其中的内容，如下图所示。



5.3.2 文件夹加密精灵

文件夹加密精灵是一款使用方便、安全可靠的文件加密软件，它具有安全性高、简单易用、界面美观的特点，可在 Windows 98/Me/2000/XP 等操作系统中使用。文件夹加密精灵的主要功能包括快速加解密、安全解加密、移动加解密、伪装/还原文件夹、隐藏/恢复文件夹、文件夹粉碎等。

基础知识

常用扫描工具

系统漏洞攻防

安全策略

系统文件加密

远程控制

木马攻击

聊天软件攻击

网页恶意代码攻击

电子邮件攻击

病毒攻击

使用电脑安全软件

黑客攻防

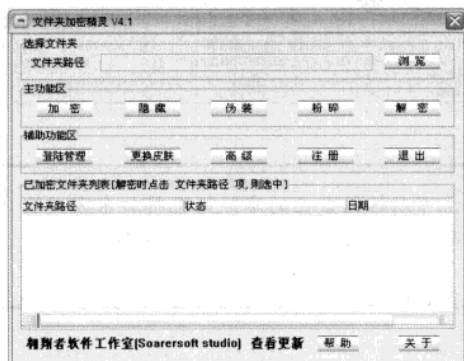
实用技巧



文件夹加密精灵使用起来非常简单，利用它对文件夹进行加密和解密的具体操作步骤如下：

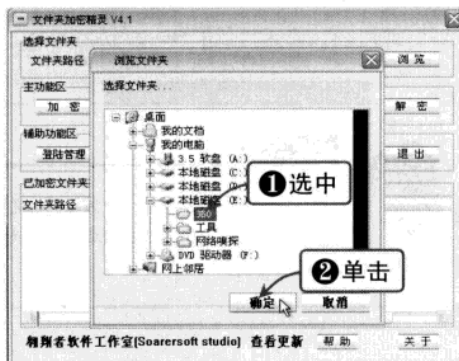
STEP 01 运行文件夹加密精灵

安装好文件夹加密精灵后，双击其运行程序图标，即可打开其工作窗口，如下图所示。



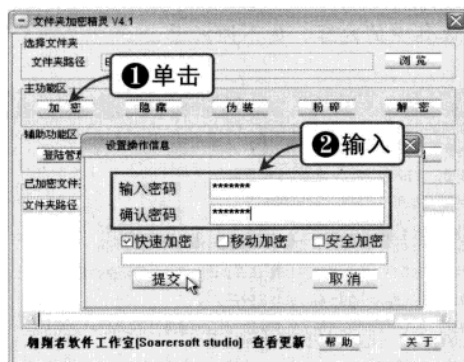
STEP 02 选择要加密的文件夹

单击“浏览”按钮，在弹出的“浏览文件夹”对话框中选择要加密的文件夹，在此选中文件夹 360，单击“确定”按钮，如下图所示。



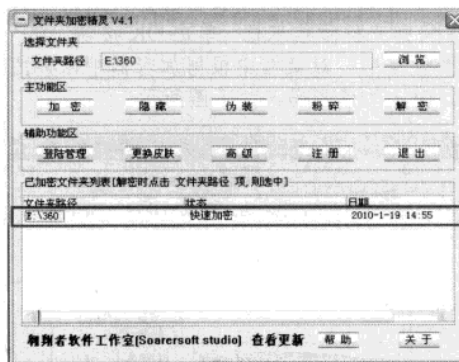
STEP 03 “设置操作信息”对话框

单击“加密”按钮，在弹出的“设置操作信息”对话框中输入密码，如下图所示。



STEP 04 对文件夹进行加密

选中“快速加密”复选框，然后单击“提交”按钮，即可在下方的已加密文件列表中看到刚刚加密的文件夹，如下图所示。



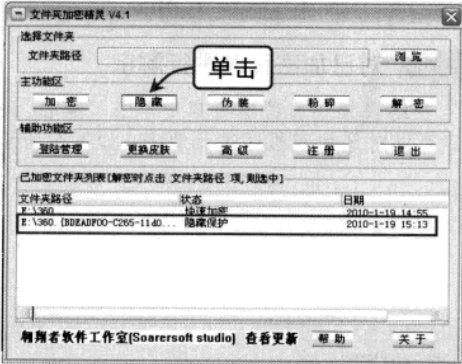
提示

在“设置操作信息”对话框中有三种不同的加密方式：“快速加密”是通过设置使用权限来加密，并且加密过的文件夹能防止删除、复制和重命名操作；“移动加密”是将文件夹中的内容做了加密，并且生成解密程序，可以独立解密；“安全加密”是采用加密算法将文件夹内各文件内容变为乱码，是对文件真正加密，适用于安全性要求极高的本机和移动存储器文件夹加密。

Chapter 05 系统与文件加密

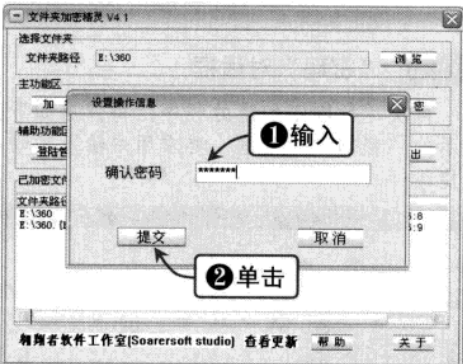
STEP 05 隐藏所选文件夹

选中刚刚加密的文件夹，单击“隐藏”按钮，即可将所选的文件夹隐藏，如下图所示。此时，在该文件夹所在的路径中将不再显示此文件夹。



STEP 06 解密文件夹

在下方的列表中选中要解密的文件夹，然后单击“解密”按钮，在弹出的“设置操作信息”对话框中输入密码，单击“提交”按钮即可解密文件夹，如下图所示。



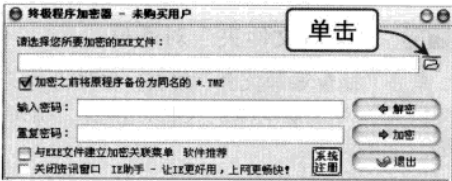
5.3.3 终极程序加密器

终极程序加密器是一款功能强大、操作简便的应用程序加锁软件。使用该软件加密过的应用程序在任何机器上运行都需要输入正确的密码。如果自己的电脑不止一个人用，而又不想他人随意使用自己安装的软件，可以利用该软件进行加密。

利用终极程序加密器对程序进行加密的具体操作步骤如下：

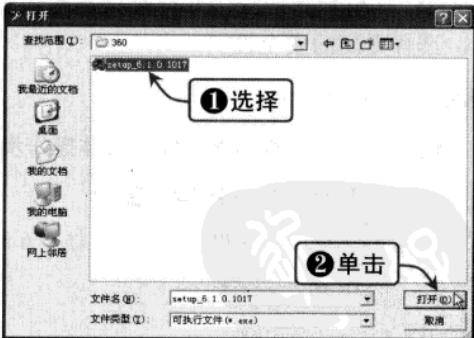
STEP 01 打开终极程序加密器

从网站下载终极程序加密器安装程序进行安装后，运行此程序，其工作窗口如下图所示，单击“打开文件”按钮。



STEP 02 选择要加密的 EXE 文件

在弹出的“打开”对话框中选择要加密的 EXE 文件，单击“打开”按钮，如下图所示。



STEP 03 输入密码

选中“加密之前将原程序备份为同名的*.TMP”复选框，然后在“输入密码”和“重复密码”文本框中输入密码，如下图所示。

STEP 04 对程序进行加密

单击“加密”按钮对程序进行加密，稍后系统会弹出如下图所示的提示信息框。

黑客

常用扫描与嗅探工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制

木马

聊天软

网页恶意

电子邮件

C盘病毒

使用电脑

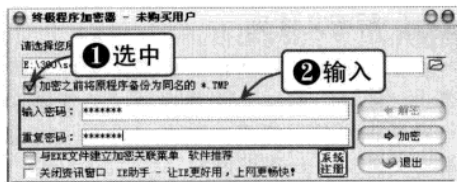
黑客攻防

实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

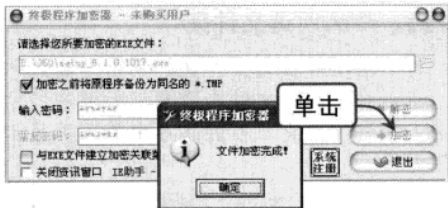


黑客攻防从新手到高手



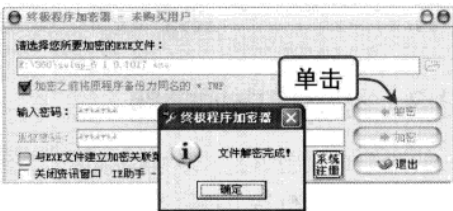
STEP 05 “密码”对话框

再次运行刚刚加密的程序，将弹出如下图所示的“密码”对话框，要求用户输入密码后方能运行。



STEP 06 对已加密程序进行解密

在终极程序加密器窗口中单击“解密”按钮，可以对已加密程序进行解密，如下图所示。



5.3.4 万能加密器

万能加密器 Easycode Boy Plus! (简称 ECBOY) 是一款功能全面、小巧高速的加密软件，它加密文件不限大小、不限文件类型，采用高速算法，加密速度快，安全性能高。该软件具有加/解密列表功能，独有的密码查询功能，还可以将加密文件编译为可执行文件，脱离 ECBOY 环境独立运行，并可对自解密文件进行分割。另外，它还可以对程序设置访问密码，具有更高的安全性。

Work1 加密文件

使用万年加密器加密文件的具体操作步骤如下：

STEP 01 打开万能加密器运行窗口

运行 Easycode Boy Plus! 程序，打开万能加密器运行窗口，如下图所示。

STEP 02 “浏览文件夹”对话框

单击“批量添加文件”按钮，在弹出的“浏览文件夹”对话框中添加文件，单击“确定”按钮，下图所示。

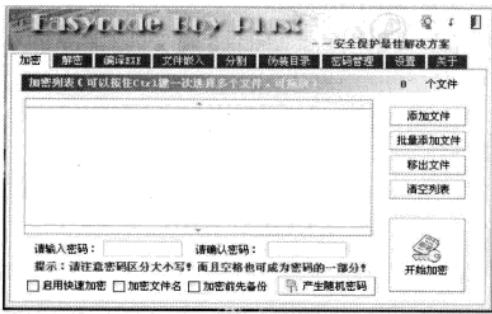


提示

使用万能加密器不仅可以对单个文件进行加密，还可以单击“批量添加文件”按钮，对多个文件进行加密。

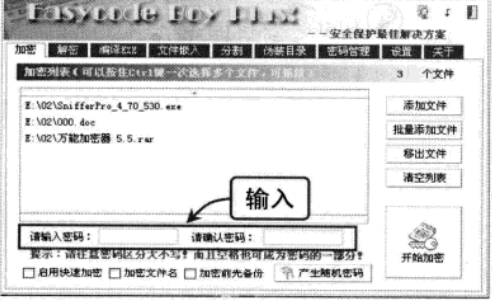
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 05 系统与文件加密



STEP 03 加密列表

此时，在加密列表中将添加该文件夹下的所有文件，在“请输入密码”和“请确认密码”文本框中输入密码，如下图所示。



STEP 05 提示信息框

单击“开始加密”按钮对文件进行加密，加密结束后将弹出提示信息框，提醒用户牢记密码，以便以后恢复，如下图所示。



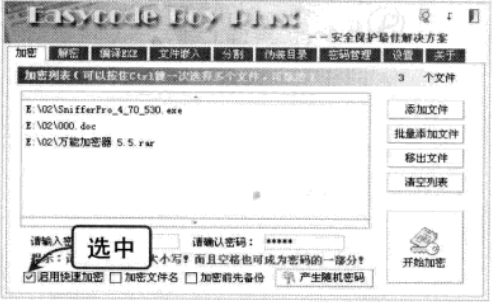
STEP 07 将已加密文件解密

在“请输入密码”文本框中输入加密密码，然后单击“开始解密”按钮，即可将已加密文件解密，如下图所示。



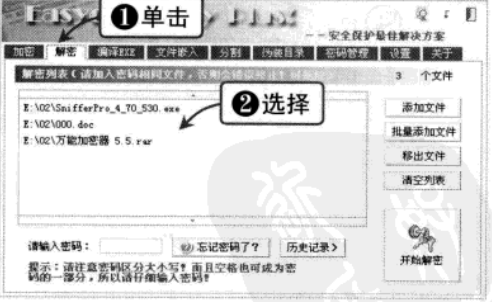
STEP 04 输入加密密码

选中“启用快速加密”复选框，如下图所示。



STEP 06 添加要解密的文件

要将原来加密的文件进行解密，可以选择“解密”选项卡，然后在解密列表中添加要解密的文件，如下图所示。



STEP 08 历史记录列表

为了便于记住密码，用户还可以单击“历史记录”按钮，在历史记录列表中保存解密记录，如下图所示。

黑客
常用扫描
与嗅探工具
系统漏洞攻击
设置系统
安全策略
系统安全
远程控制
木马
聊天软
网页恶意
代码攻击
C盘病毒
使用电脑
黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

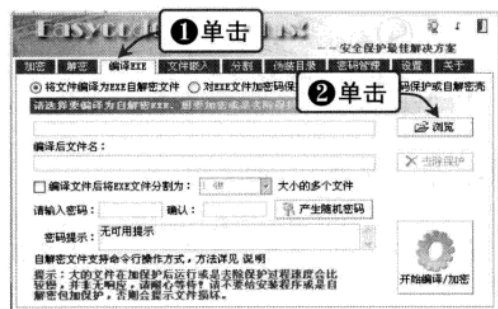


Work2 编译 EXE 文件

使用万年加密器编译 EXE 文件的具体操作步骤如下：

STEP 01 编译 EXE 界面

若要对 EXE 文件进行编译，可以单击“编译 EXE”选项卡，选择编译 EXE 界面，单击“浏览”按钮，如下图所示。



STEP 02 选择软件安装程序

弹出“打开”对话框，在该对话框中选择软件安装程序（EXE 文件），单击“打开”按钮，如下图所示。



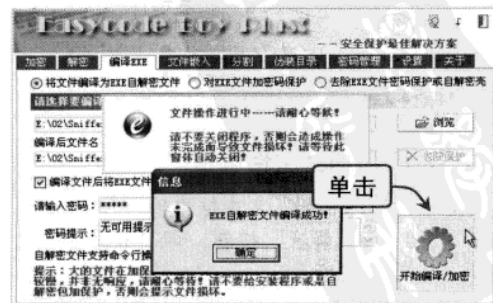
STEP 03 编译后分割文件

在下方选中“编译文件后将 EXE 文件分割为”复选框，并在后面的数值框中设置分割文件大小，如下图所示。



STEP 04 对文件进行编译并分割

在“请输入密码”和“确认”文本框中输入编译密码，然后单击“开始编译/加密”按钮，即可对文件进行编译并分割，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

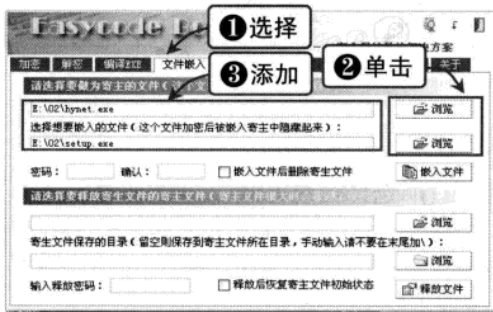
Chapter 05 系统与文件加密

Work3 嵌入与分割文件

使用万年加密器嵌入与分割文件的具体操作步骤如下：

STEP 01 添加寄主文件和嵌入文件

在万能加密器工作窗口中选择“文件嵌入”选项卡，单击“浏览”按钮，添加寄主文件和嵌入文件，如下图所示。



STEP 02 嵌入文件

在“密码”和“确认”文本框中输入密码，并选中“嵌入文件后删除寄主文件”复选框，单击“嵌入文件”按钮，即可将文件嵌入，如下图所示。



STEP 03 添加寄主文件

要解除嵌入，可以单击下面的“浏览”按钮添加寄主文件（已嵌入文件），设置释放目录，并输入释放密码，如下图所示。



STEP 04 释放文件

选中“释放后恢复寄主文件初始状态”复选框，然后单击“释放文件”按钮释放文件，效果如下图所示。



STEP 05 添加要分割的文件

要对文件进行分割，可先选择“分割”选项卡，然后单击“打开”按钮，添加要分割的文件，单击“浏览”按钮设置切割后文件的存放目录，如下图所示。

STEP 06 分割文件

在“分割选项”选项区中定义分割文件的大小，然后单击“开始分割”按钮，对文件进行分割，效果如下图所示。



提示

通过分割文件可以将原来体积很大的文件分割为很小的多个文件，这样便于在网络上快速传输，很多黑客高手都是通过这种方式对后门程序进行分割隐藏的。

黑客
常用扫描
与嗅探工具
Windows系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
网页恶
意
代码攻
防
电子邮
件攻
防
C盘病
使用电
脑
黑客攻
防



Work4 伪装文件目录

使用万年加密器还可以对文件进行伪装，其具体操作步骤如下：

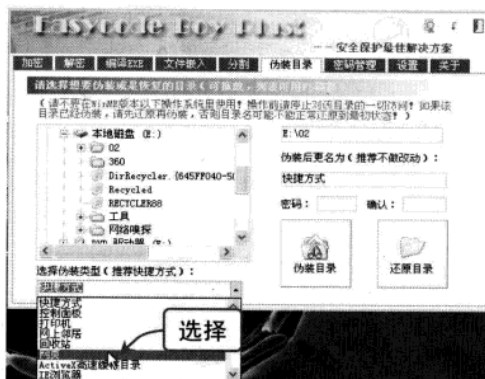
STEP 01 选择要伪装的文件夹

在万年加密器工作窗口中选择“伪装目录”选项卡，选择要伪装的文件夹，如下图所示。



STEP 02 选择伪装方式

在“选择伪装类型”下拉列表框中选择伪装方式，在此选择“网页”选项，如下图所示。



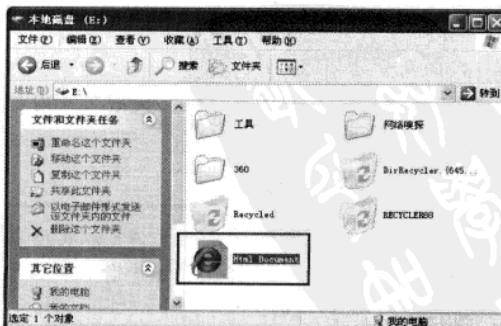
STEP 03 对文件夹进行伪装

在“密码”和“确认”文本框中输入密码，然后单击“伪装目录”按钮，对文件夹进行伪装，如下图所示。



STEP 04 文件夹变为网页形式

伪装操作结束后，打开此文件夹所在窗口，即可看到该文件夹变为网页形式，效果如下图所示。



5.4 破解管理员账户

在 Windows XP 操作系统中，管理员账户有着极大的控制权限，黑客常常利用各种技术对该账户进行破解，从而获得电脑的控制权。

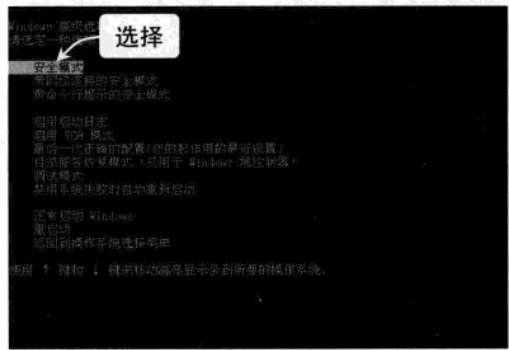
5.4.1 使用 Administrator 账户登录

每台电脑装上 Windows XP 操作系统后，除了用户自己新建的账户外，还会自动创建一个名为 Administrator 的管理电脑的内置账户，它平时是隐藏的，拥有电脑管理的最高权限，新建的账户都是在它下面派生的。

在不知道用户登录密码的情况下，可以使用 Administrator 账户登录，具体操作方法如下：

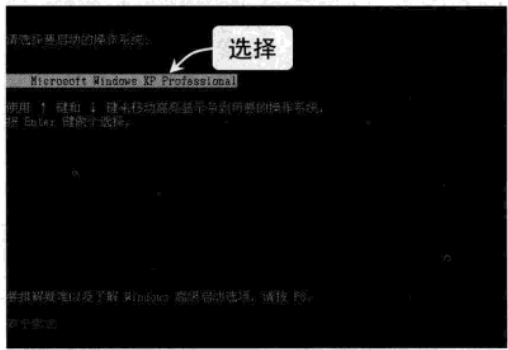
STEP 01 “Windows 高级选项菜单”界面

首先启动电脑，在出现开机画面后按下【F8】键，进入“Windows 高级选项菜单”界面，在该界面中选择“安全模式”选项，如下图所示。



STEP 02 选择要启动的操作系统

按【Enter】键，进入“请选择要启动的操作系统”界面，选择 Microsoft Windows XP Professional 选项，如下图所示。



STEP 03 系统登录界面

按【Enter】键，启动 Windows XP 操作系统，进入系统登录界面，此时会看到 Administrator 账户，如下图所示。



STEP 04 进入安全模式下的系统环境

单击 Administrator 账户，在弹出的文本框中输入密码（如系统没有设置密码，可直接进入系统），按【Enter】键即可进入系统，如下图所示。



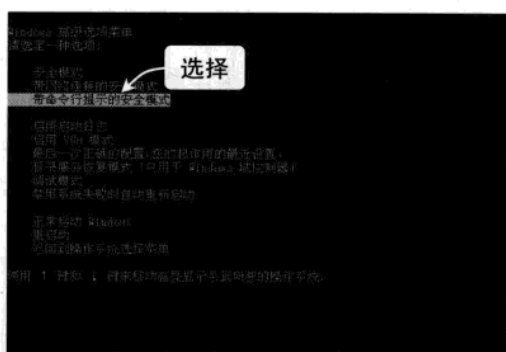


5.4.2 强制清除管理员密码

在 Windows XP 中提供了 net user 命令，利用该命令可以添加、修改用户账户信息，现在以恢复本地用户 li 的口令为例，来介绍解决忘记登录密码问题的方法。

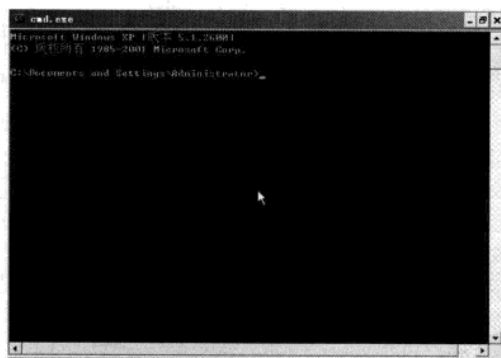
STEP 01 “Windows 高级选项菜单”界面

首先启动电脑，在出现开机画面后按【F8】键，进入“Windows 高级选项菜单”界面，在该界面中选择“带命令行提示的安全模式”选项，如下图所示。



STEP 02 进入命令行模式

运行过程结束后，列出了系统超级用户 Administrator 和本地用户 li 的选择菜单，单击 Administrator，进入命令行模式，如下图所示。



STEP 03 键入强制更改口令的命令

键入命令：net user li 123456 /add，强制将 li 用户的口令更改为 123456，如下图所示。



STEP 04 登录系统

重新启动电脑，选择正常模式下运行，即可用更改后的口令 123456 登录 li 用户，如下图所示。



5.4.3 创建密码恢复盘

人的记忆力并不是非常可靠的，谁都有忘记密码的时候。Windows XP 自带创建账号密码恢复盘功能，利用该功能可以创建密码恢复盘，以便用户忘记账户密码后进行恢复。创建密码恢复盘的具体操作步骤如下：

Chapter 05 系统与文件加密

STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“用户账户”图标，如下图所示。



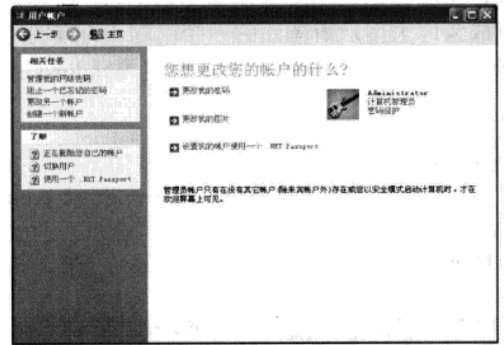
STEP 02 打开“用户账户”窗口

打开“用户账户”窗口，如下图所示。



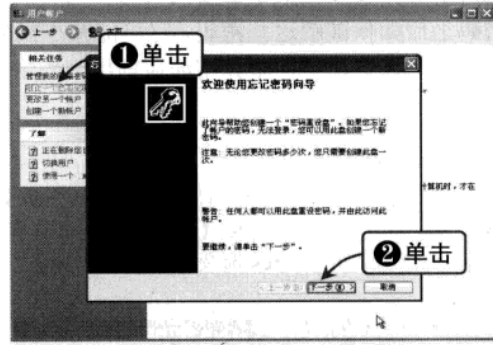
STEP 03 “您想要更改您的账户的什么？”窗口

单击要创建密码恢复盘的账户，打开“您想要更改您的账户的什么？”窗口，如下图所示。



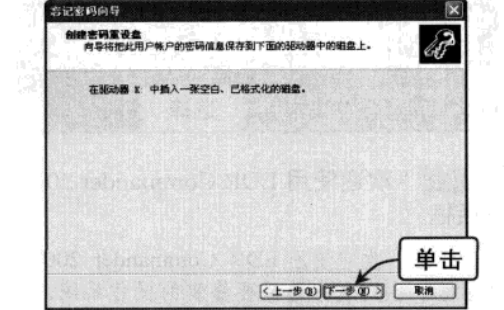
STEP 04 “忘记密码向导”对话框

单击“阻止一个已忘记的密码”超链接，弹出“忘记密码向导”对话框，单击“下一步”按钮，如下图所示。



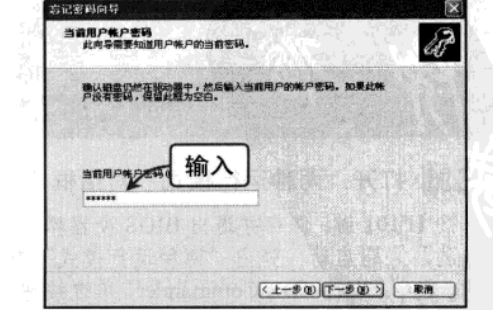
STEP 05 “创建密码重设盘”界面

此时，弹出“创建密码重设盘”对话框，单击“下一步”按钮，如下图所示。



STEP 06 输入当前用户密码

弹出“当前用户账户密码”对话框，在下面的文本框中输入当前用户密码，如下图所示。



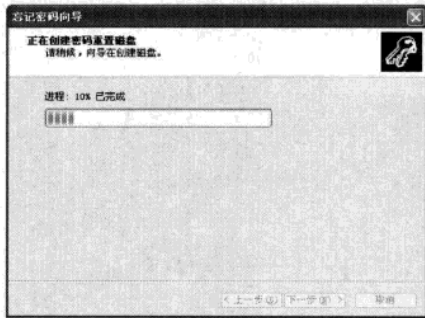
黑客
基础知识
常用扫描
与嗅探工具
Windows 系统
漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
件攻防
网页恶
意代码
攻击防
电子邮
件攻防
病毒防
使用电
脑安全
软件
黑客攻
防技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



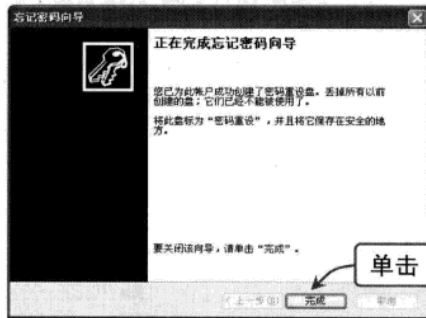
STEP 07 开始创建密码重置盘

单击“下一步”按钮，开始创建密码重置盘，如下图所示。



STEP 08 密码重置盘创建完毕

当对话框中显示进程完成后，单击“下一步”按钮，弹出如下图所示的对话框，单击“完成”按钮，即可完成密码重置盘的创建。

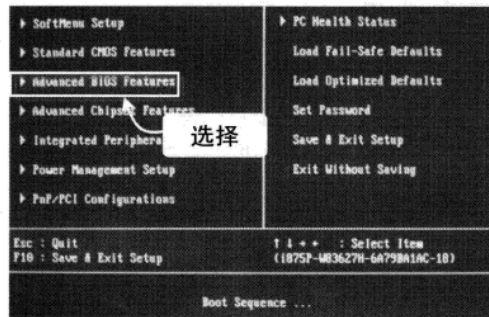


5.4.4 使用密码恢复软件

在日常的电脑操作中，我们随时随地都离不开密码——进入 BIOS 设置程序要用 CMOS 密码、进入 Windows 要使用用户密码、编辑 Word 文档要设置文档密码……，所有这些都为用户的数据安全提供了必要的安全保障。不过谁也无法保证自己绝对不会忘记密码，在忘记密码之后如何破解这些密码，尽可能减少损失就成为广大用户所关注的一个问题。为方便用户的使用，下面将简单介绍如何使用密码恢复软件 ERD Commander 2005 恢复 Windows 系统管理员密码。

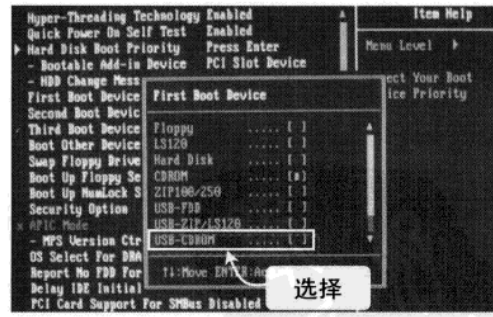
STEP 01 进入 BIOS

启动电脑，在电脑开始自检时按住【Delete】键不放，可进入 BIOS，按【↓】键，向下选择 Advanced BIOS Features 选项，如下图所示。



STEP 02 设置从光驱启动

按【Enter】键进入 BIOS 设置界面，按【↓】键，向下选择 First Boot Device 选项，并按【Enter】键进入设置界面，向下移动光标，选择 USB-CDROM 选项，如下图所示。



STEP 03 打开“两种运行模式”对话框

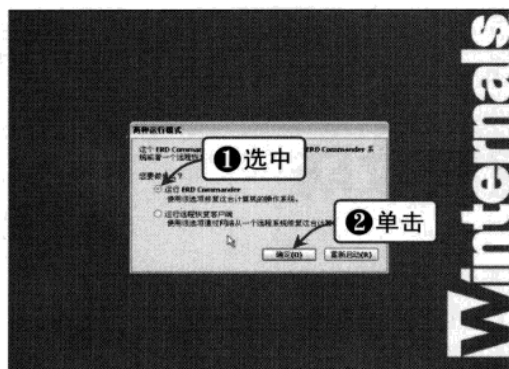
按【F10】键，保存并退出 BIOS 设置界面，让电脑从光驱启动，弹出“两种运行模式”对话框。选中“运行 ERD Commander”单选按钮，单击“确定”按钮，如下图所示。

STEP 04 “欢迎使用 ERD Commander 2005”对话框

弹出“欢迎使用 ERD Commander 2005”对话框，在列表中选择要修复的操作系统，然后单击“确定”按钮，如下图所示。

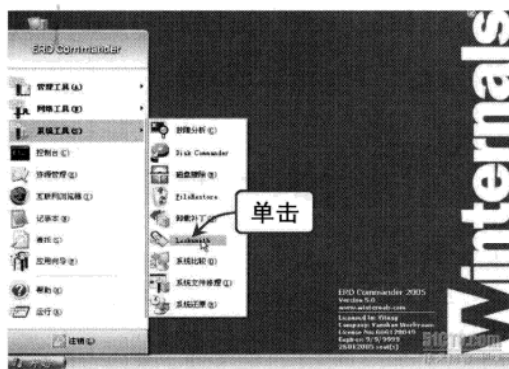
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 05 系统与文件加密



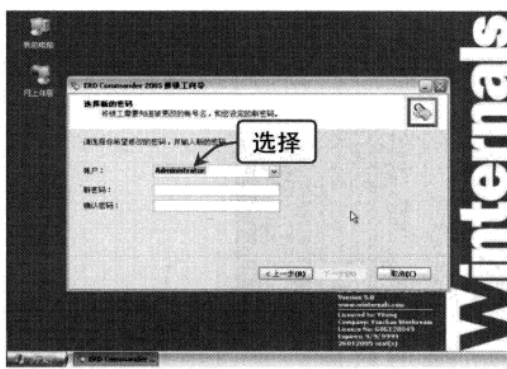
STEP 05 进入 EDR Commander 主界面

进入 EDR Commander 主界面，单击“开始”|“系统工具”|Locksmith 命令，如下图所示。



STEP 06 输入当前用户密码

弹出“EDR Commander 修锁工向导”对话框,在下面的下拉列表框中选择要重设密码的账户,在此选择 Administrator 账户,如下图所示。



提示

在“新密码”和“确认密码”文本框中输入密码，然后单击“下一步”按钮，在弹出的对话框中单击“完成”按钮，即可重设 Windows 系统管理员密码。

Chapter

06

远程控制攻防

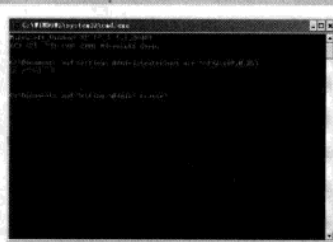
黑客攻击目标的最终目的就是拿到对方的控制权，能够实现远程控制主机，通过网络对远程计算机的系统设置进行修改。本章将讲解一些黑客进行远程入侵的方法，并简单介绍几个实现远程控制的途径。

本章建议学习时间：

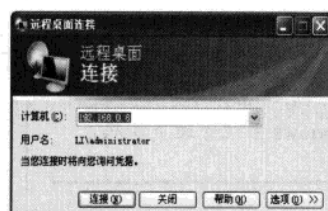
本章建议学习时间为 60 分钟，其中分配 35 分钟学习远程控制攻防的相关知识，25 分钟观看教学视频并进行练习。

学完本章后您可以：

- 了解基于认证入侵方法
- 了解通过注册表入侵方法
- 使用 Windows XP 远程控制
- 使用网络执法官
- 使用远程控制软件



建立 IPC\$ 连接



输入目标主机的 IP 地址



打开网络执法官

重要知识点视频索引



6.1 基于认证入侵

如果黑客能够与用户的电脑建立基于认证的远程连接，那他们就可以不使用任何入侵工具完全地控制用户的电脑，轻松地在用户的电脑上随意操作。

6.1.1 IPC\$入侵与防范

IPC\$是 Windows 系统特有的一项管理功能，是微软公司为了方便用户使用计算机而设计的，主要用来远程管理计算机。但事实上使用这个功能最多的人不是网络管理员，而是“入侵者”，他们通过建立 IPC\$连接与远程主机实现通信，在远程计算机上建立、复制或删除文件，在远程计算机上执行命令。

Work1 什么是 IPC\$入侵

IPC 是 Windows 操作系统提供的一个通信基础，用来在两台计算机进程之间建立通信连接，而 IPC 后面的“\$”是 Windows 系统所使用的隐藏符号，因此“IPC\$”表示 IPC 共享，但为隐藏的共享。

IPC\$是 Windows NT 及 Windows 2000/XP/2003 特有的一项功能，通过这项功能，一些网络程序的数据交换可以建立在 IPC 上面，实现远程访问和管理计算机。通俗些来说，IPC 连接就像是挖好的地道，通信程序就通过这个 IPC 地道访问目标主机。默认情况下 IPC\$是共享的，除非手动删除 IPC\$。通过 IPC\$连接，入侵者就能够远程控制目标主机。因此，这种基于 IPC\$的入侵也常常被简称为 IPC\$入侵。

Work2 IPC\$入侵方式

为了配合 IPC 共享工作，Windows 操作系统（不包括 Windows 98 系列）在安装完成后，自动设置共享的目录为 C 盘、D 盘、E 盘、ADMIN 目录（C:\WINNT\）等，即为 ADMIN\$、C\$、D\$、E\$等，但要注意这些共享是隐藏的，只有管理员能够对它们进行远程操作。在 MS-DOS 环境中输入 net share 命令，可以查看本机共享资源。

通过 IPC\$连接进行入侵的条件是已获得目标主机管理员的账号和密码，下面用实例来介绍如何建立和断开 IPC\$连接，看看入侵者是如何将远程磁盘映射到本地的，通过了解这些知识，这样用户就能有效地防止他人入侵本机。



提示

要打开目标的 IPC\$，首先需要获得一个不依赖于 IPC\$的 shell，如 sql 的 cmd 扩展、telnet、木马。当然，这 shell 必须是 admin 权限的，然后用户可以使用 shell 执行命令 net share IPC\$ 来开放目标的 IPC\$。

STEP 01 输入 cmd 命令

单击“开始”|“运行”命令，弹出“运行”对话框，在“打开”文本框中输入 cmd 命令，单击“确定”按钮，如下图所示。

STEP 02 建立 IPC\$连接

打开“命令提示符”窗口，输入命令 net use \\192.168.0.253，如下图所示。

基础知识
黑客

常用扫描
与嗅探工具

Windows 系
统漏洞攻防

设置系统
安全策略

系统与文
件加密

远程控
制攻防

木马
攻防

聊天软
件攻防

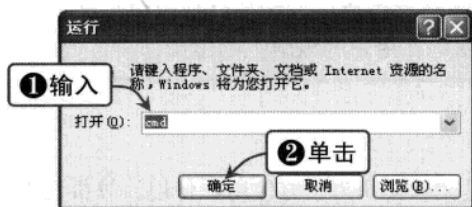
网页恶
意代码攻防

电子邮
件攻防

C 盘病
毒攻防

使用电
脑安全软件

黑客攻
防实用技巧



STEP 03 映射网络驱动器

输入 `net use \\192.168.0.253\c$` 命令，命令执行成功后输入用户名和密码，即可映射网络驱动器，如下图所示。



STEP 04 断开连接

输入 `net use * /del` 命令，可断开所有 IPC\$ 连接，其中“*”表示所有的连接，如下图所示。



提示

“\\192.168.0.253\c\$”表示目标主机 192.168.0.253 上的 C 盘，其中“\$”符号表示隐藏的共享；“z:”表示将远程主机的 C 盘映射为本地磁盘的盘符。该命令表示把 192.168.0.253 这台目标主机上的 C 盘映射为本地的 Z 盘，映射成功后，打开“我的电脑”窗口，会发现多出一个 Z 盘，上面写着“C\$位于 192.168.0.253 上”，该磁盘即为目标主机的 C 盘。

Work3 创建后门账号

黑客还可以利用 IPC\$ 入侵创建后门账号，下面对其方式进行简单介绍。首先，需要用户了解以下知识：

（1）什么是 BAT 文件

BAT 文件是在 Windows 系统中的一种文件格式，称为批处理文件。简单来说，就是把需要执行的一系列 DOS 命令按顺序先后写在一个后缀名为 BAT 的文本文件中。通过鼠标双击或 DOS 命令执行该 BAT 文件，就相当于执行一系列 DOS 命令。

（2）什么是计划任务

举个例子，假设想在明天上午 10 点给电脑杀毒，但是正好明天上午 10 点要出去办事，那怎么办呢？这时候就要使用“计划任务”这个功能，令计算机在明天上午 10 点自动执行杀毒程序。计划任务是 Windows 系统自带的功能，可以在控制面板中找到。除此之外，还可能用命令行的方式来添加计划任务。

Chapter 06 远程控制攻防

（3）涉及的相关 DOS 命令

copy 命令。把一个文件复制到另一个地方，“另一个地方”可以是本地计算机的目录、磁盘，也可以是另一台主机的目录或磁盘。

at 命令。用来建立计划任务。

net time 命令。用来查看目标计算机的系统时间，以便使用计划任务指定时间。

net user 命令。用来管理计算机上面的账号，其中：

- ❖ 查看账号命令：net user。
- ❖ 建立账号命令：net user name passwd/add。
- ❖ 删除账号命令：net user name passwd/del。

net localgroup 命令。用来管理工作组。

（4）操作方法

步骤一：编写 BAT 文件。打开记事本，输入 net user sysbak 123456 /add 和 net localgroup administrators sysback /add 命令，然后把该文件另存为 hack.bat。

步骤二：与目标主机建立 IPC\$连接。在上面的实例中已经介绍过这一步骤，所以在此省略。

步骤三：复制文件至目标主机。打开 MS-DOS，输入 copy hack.bat \\192.168.27.128\c\$ 命令，copy 命令执行成功后，就已经把 D 盘下的 hack.bat 文件复制到 192.168.27.128 的 C 盘内。此外，也可以在图形界面下把 hack.bat 复制、粘贴到目标主机中。

步骤四：通过计划任务使远程主机执行 hack.bat 文件。打开 MS-DOS，输入 net time \\192.168.27.128 命令。假设回显的目标系统时间为 13:33，然后根据该时间为远程主机建立计划任务。输入 at\\192.168.27.128 13:45 c:\hack.bat 命令，该命令表示在下午 13 点 45 分执行目标主机 C 盘中的 hack.bat 文件。计划任务添加完毕后，使用命令 net use * /del 断开 IPC\$ 连接。

步骤五：验证账号是否成功建立。等待一段时间后，估计远程主机已经执行了 hack.bat 文件。通过建立 IPC\$连接来验证是否成功建立 sysback 账号。如果连接成功，说明管理员账号 sysback 已经成功建立。

Work4 IPC\$入侵防范

IPC\$为入侵者远程连接目标主机提供了可能，入侵者所使用的工具中有很多是基于 IPC\$来实现的。IPC\$在为管理员们提供了方便操作的同时，也留下了严重的安全隐患。因此，如果成功地阻止了 IPC\$入侵，也就阻挡了相当一部分入侵者。

1. 删除默认共享

要阻止 IPC\$入侵，可以通过删除默认共享来实现，其具体操作步骤如下：

STEP 01 弹出“网络连接”窗口

在桌面上的“网上邻居”图标上右击，在弹出的快捷菜单中选择“属性”选项，弹出“网络连接”窗口，如下图所示。在“本地连接”图标上右击，在弹出的快捷菜单中选择“属性”选项。

STEP 02 弹出“本地连接 属性”对话框

弹出“本地连接 属性”对话框，在下面列表框中取消选择“Microsoft 网络的文件和打印机共享”、NWLink NetBIOS 和 NWLink IPX/NetBIOS Compatible Transport 等复选框，如下图所示。

基础
知识

与嗅探工具
常用扫描

系统漏洞攻防
Windows系

安全策略
设置系统

系统安全
件加密

远程控制
制攻防

木马
攻防

聊天软
件攻防

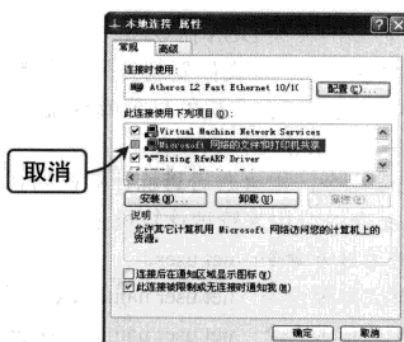
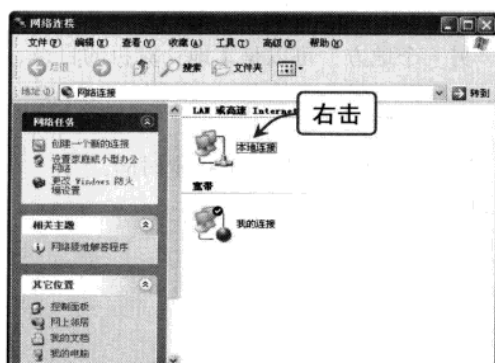
网页恶
意代码防

电子邮
件攻防

C盘病
毒攻防

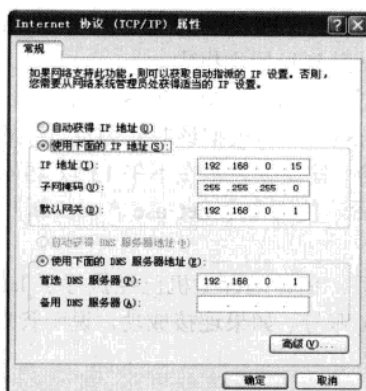
使用电
脑安全软

黑客攻
防实用技



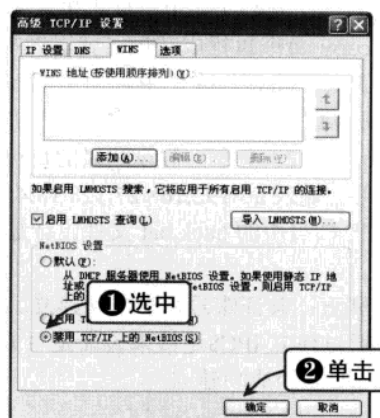
STEP 03 打开“Internet 协议 (TCP/IP) 属性”对话框

选择“Internet 协议 (TCP/IP)”选项，再单击“属性”按钮，弹出“Internet 协议 (TCP/IP) 属性”对话框，如下图所示。



STEP 04 打开“高级 TCP/IP 设置”对话框

单击“高级”按钮，打开“高级 TCP/IP 设置”对话框，选择 WINS 选项卡，选中“禁用 TCP/IP 上的 NetBIOS”单选按钮，如下图所示。单击“确定”按钮，即可应用设置。



提示



用户还可以通过批处理文件来处理上述问题，其命令格式为：
@echo off
net share c\$ /del net share d\$ /del net share e\$ /del net share f\$ /del net share
ADMIN\$ /del.

2. 禁止空连接进行枚举攻击

有了 IPC\$ 空连接作为连接基础，入侵者可以反复进行试探性连接，直到连接成功、获取密码。IPC\$ 为入侵者通过暴力破解来获取远程主机管理员密码提供了可能性，被入侵只是时间问题。禁止空连接进行枚举攻击的具体方法如下：

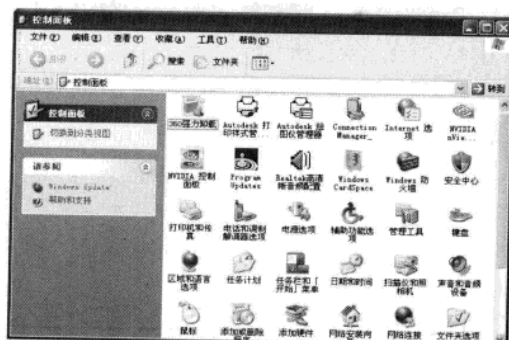
STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，如下图所示。

STEP 02 打开“管理工具”窗口

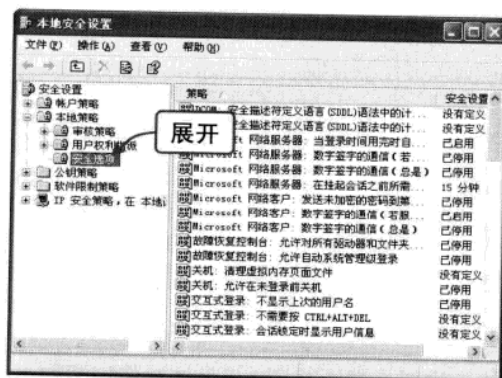
打开“管理工具”窗口，在“管理工具”窗口中双击“本地安全策略”图标，如下图所示。

Chapter 06 远程控制攻防



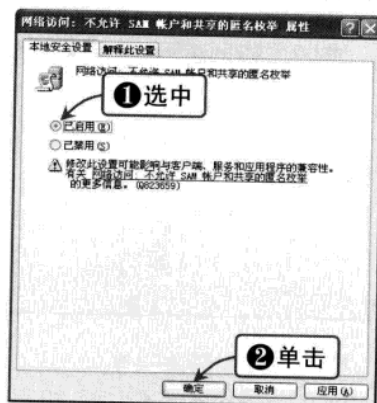
STEP 03 打开“本地安全设置”窗口

打开“本地安全设置”窗口，然后依次展开“安全设置”|“本地策略”|“安全选项”选项，如下图所示。



STEP 04 启用安全策略

双击右侧窗格中的“网络访问：不允许 SAM 账户和共享的匿名枚举”策略，在打开的对话框中选中“已启用”单选按钮，如下图所示。单击“确定”按钮应用设置，即可完成操作。



3. 关闭 Server 服务

Server 服务是 IPC\$ 和默认共享所依赖的服务，如果关闭 Server 服务，IPC\$ 和默认共享便不存在，但同时也使服务器丧失其他一些服务功能，因此该方法不适合服务器使用，只适合个人计算机使用。关闭 Server 服务的具体操作步骤如下：

STEP 01 打开“控制面板”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，如下图所示。

STEP 02 打开“管理工具”窗口

打开“管理工具”窗口，双击“服务”图标，如下图所示。



提示

Server 服务支持此计算机通过网络的文件、打印和命名管道共享。如果服务停止，这些功能不可用。如果服务被禁用，任何直接依赖于此服务的程序将无法启动。

基础知识

与嗅探工具

系统漏洞攻防

安全策略

系统与安全

远程控制

木马

聊天软件

网页恶意

代码攻防

电子战

攻击

使用电脑

黑客攻防

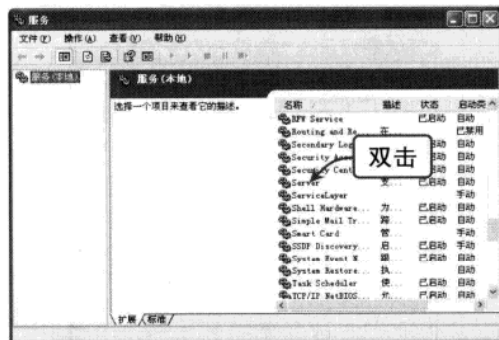
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



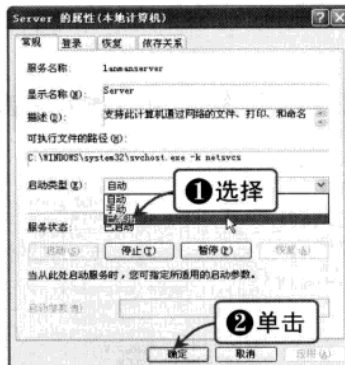
STEP 03 打开“服务”窗口

打开“服务”窗口，如下图所示。在服务列表中找到 Server 服务，双击该服务，



STEP 04 禁用 Server 服务

在弹出的对话框中选择“已禁用”选项，如下图所示。确认上述操作，单击“确定”按钮，并重新启动计算机，即可禁用 Server 服务。

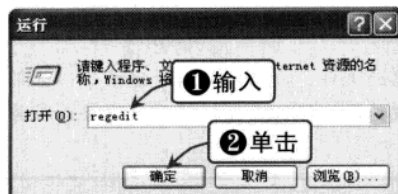


4. 修改注册表禁止共享

在 Windows XP 操作系统中，用户可以通过修改注册表禁止共享，其具体操作步骤如下：

STEP 01 输入 regedit 命令

单击“开始”|“运行”命令，弹出“运行”对话框，在“打开”下拉列表框中输入 regedit 命令，单击“确定”按钮，如下图所示。



STEP 02 打开“注册表编辑器”窗口

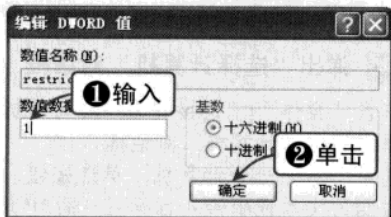
打开“注册表编辑器”窗口，然后依次展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 分支，如下图所示。



Chapter 06 远程控制攻防

STEP 03 打开“本地安全设置”窗口

双击右侧窗格中的 restrictanonymouse 键，弹出“编辑 DWORD 值”对话框，然后将“数值数据”文本框中的数值修改为 1（如下图所示），单击“确定”按钮应用设置。



STEP 04 启用安全策略

在“注册表编辑器”窗口中依次展开 HK-KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 分支，如下图所示。



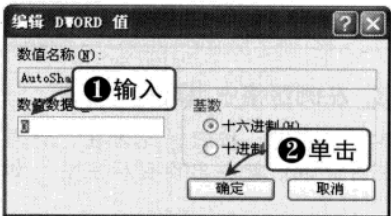
STEP 05 新建 DWORD 值

在右侧窗格的空白区域右击，在弹出的快捷菜单中选择“新建”|“DWORD 值”选项，如下图所示。



STEP 06 完成设置

创建一个名为 AutoShareServer 的键值项，然后双击该键值，弹出“编辑 DWORD 值”对话框，设置其键值为 0，单击“确定”按钮，如下图所示。



6.1.2 Telnet 入侵概述

虽然 IPC\$ 连接也能远程执行命令，但相比之下，Telnet 对入侵者而言会更方便。入侵者利用 Telnet 从一个“肉鸡”（就是被黑客攻破，种植了木马病毒的电脑，黑客可以随意操纵它，并利用它做任何事情）登录到另一个“肉鸡”，这样在入侵过程中就很好地隐藏了自己的 IP 地址。要进行 Telnet 入侵，首先要开启目标主机上的 Telnet 服务，具体操作步骤如下：

STEP 01 输入 cmd 命令

单击“开始”|“运行”命令，弹出“运行”对话框，在“打开”下拉列表框中输入 cmd 命令，如下图所示。

STEP 02 建立 IPC\$ 连接

打开“命令提示行”窗口，然后使用 net use\\192.168.0.8\ipc\$ “123456”/user: “li” 命令，建立 IPC\$ 连接，如下图所示。

黑客
常用扫描
与嗅探工具
系统安全
安全策略
系统加密
远程控制
木马
聊天软件
网页恶意
代码攻击
电子邮件
C 盘病毒
使用电脑
安全软件
黑客攻防

STEP 04 弹出“选择计算机”对话框

选中“另外一台计算机”单选按钮，然后在右侧的文本框中输入目标主机的 IP 地址，如下图所示。

STEP 05 左侧窗格中出现目标主机

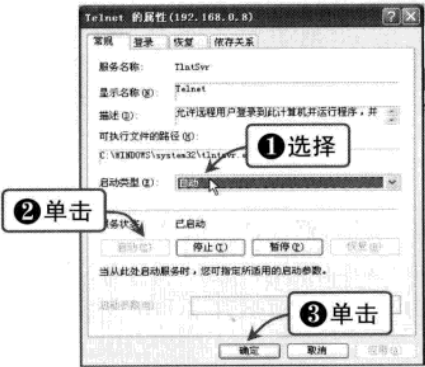
STEP 06 双击“Telnet”选项

依次展开“服务和应用程序”|“服务”选项，在右侧窗格中双击 Telnet 选项，如下图所示。

Chapter 06 远程控制攻防

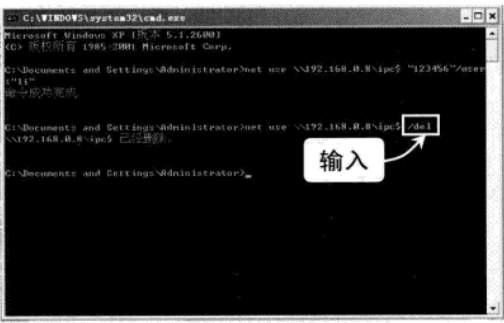
STEP 07 启用 Telnet 服务

弹出“Telnet 的属性 (192.168.0.8)”对话框，在“启动类型”下拉列表框中选择“自动”选项，依次单击“应用”和“启动”按钮，激活此项服务，然后单击“确定”按钮应用设置，如下图所示。



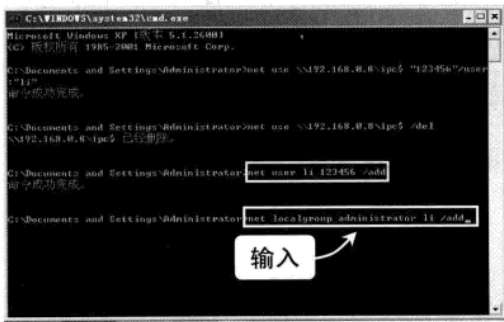
STEP 08 断开 IPC\$ 连接

在“命令提示符”窗口中使用 del 命令断开 IPC\$ 连接，如下图所示。



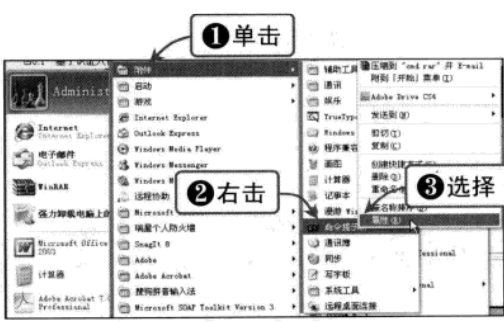
STEP 09 打开“新规则 属性”对话框

在“命令提示符”窗口中分别执行命令 net user li 123456/add 和 net localgroup administrator li/add，如下图所示。



STEP 10 “IP 筛选器列表”对话框

单击“开始”|“所有程序”|“附件”命令，在展开菜单中右击“命令提示符”选项，在弹出的快捷菜单中选择“属性”选项，如下图所示。



提示

除了上述方法外，用户还可以在命令提示符窗口图标上右击，然后在弹出的菜单中选择“属性”选项，这样同样也可以进入“命令提示符 属性”窗口。

STEP 11 打开“命令提示符 属性”对话框

打开“命令提示符 属性”对话框，选择“快捷方式”选项卡，然后单击“高级”按钮，如下图所示。

STEP 12 以其他用户身份运行

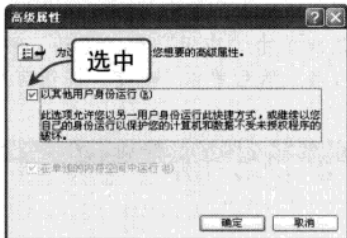
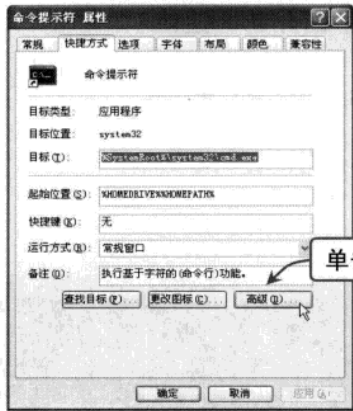
弹出“高级属性”对话框，在该对话框中选中“以其他用户身份运行”复选框，依次单击“确定”按钮应用设置，如下图所示。

- 黑客
- 常用扫描
- 与嗅探工具
- 系统漏洞攻防
- 安全策略
- 系统与文
- 件加密
- 远程控制
- 木马
- 聊天软
- 网页恶
- 件攻击
- 电子邮
- 病毒防
- 使用电
- 黑客攻

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

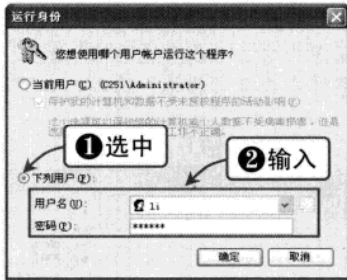


黑客攻防从新手到高手



STEP 13 打开“运行身份”对话框

单击“开始”|“所有程序”|“附件”|“命令提示符”命令，弹出“运行身份”对话框，选中“下列用户”单选按钮，在“用户名”下拉列表中输入已创建的账号，在“密码”文本框中输入密码，单击“确定”按钮，如下图所示。



STEP 14 “筛选器操作”选项卡

弹出“命令提示符”窗口，然后输入“telnet 192.168.0.8”命令即可进行 Telnet 登录，如下图所示。



6.2 通过注册表入侵

Windows 注册表是帮助系统控制硬件、软件、用户环境和 Windows 界面的一套数据文件。注册表保存关于缺省数据和辅助文件的位置信息、菜单、按钮条、窗口状态和其他可选项。它同样也保存了安装信息、安装软件的用户、软件版本号和日期、序列号等，根据安装软件的不同，它包括的信息也各不相同。

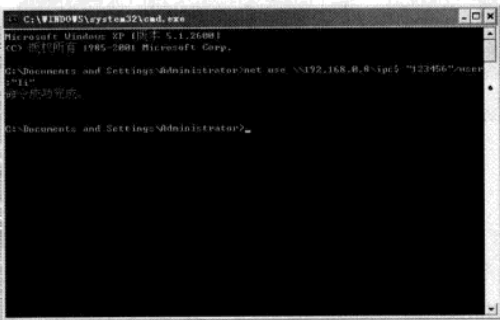
6.2.1 开启远程注册表服务

如果要想连接远程计算机的“网络注册表”实施入侵的话，除了能够成功建立 IPC\$ 连接以外，还需要在远程计算机上开启“远程注册表服务”功能。开启远程注册表服务的具体操作方法如下：

Chapter 06 远程控制攻防

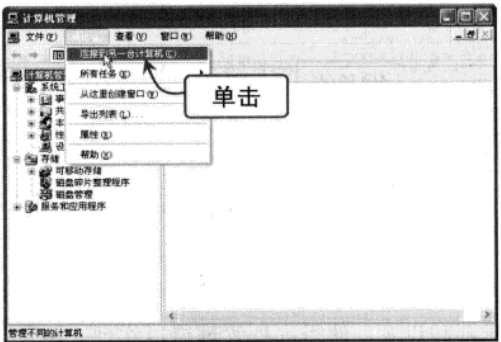
STEP 01 与远程主机建立 IPC\$ 连接

打开“命令提示符”窗口，使用 IPC\$ 命令与远程主机建立 IPC\$ 连接，如下图所示。



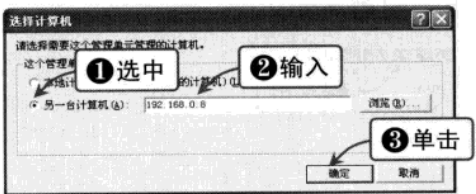
STEP 02 “连接到另一台计算机”命令

在桌面上的“我的电脑”图标上右击，在弹出的快捷菜单中选择“管理”选项，打开“计算机管理”窗口，然后单击“操作”|“连接到另一台计算机”命令，如下图所示。



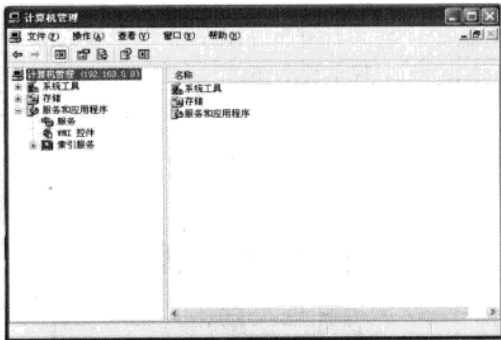
STEP 03 弹出“选择计算机”对话框

弹出“选择计算机”对话框，选中“另一台计算机”单选按钮，然后在其右侧的文本框中输入目标主机的 IP 地址，单击“确定”按钮，如下图所示。



STEP 04 看到目标主机的名称

返回“计算机管理”窗口，此时在左侧的窗格中可以看到目标主机的名称，如下图所示。



STEP 05 激活远程注册表服务

依次展开“服务和应用程序”|“服务”选项，双击右侧窗格中的 Remote Registry 选项，弹出其属性对话框，在“启动类型”下拉列表框中选择“自动”选项，然后依次单击“应用”和“启动”按钮激活此项服务，如下图所示。

STEP 06 断开 IPC\$ 连接

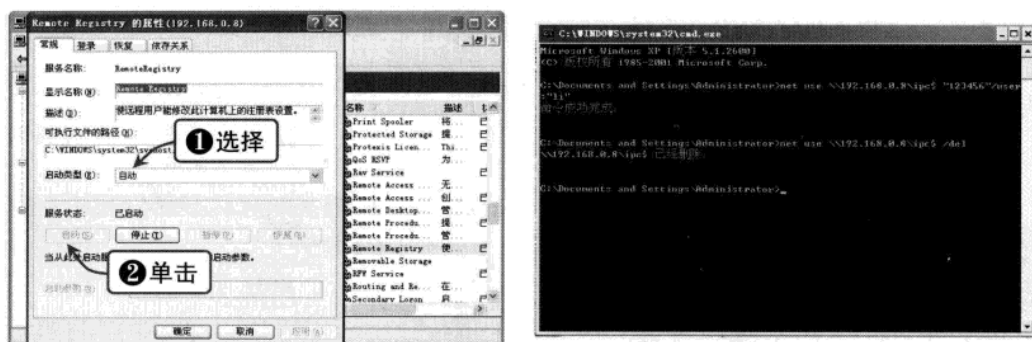
单击“确定”按钮应用设置，关闭“计算机管理”窗口，然后断开 IPC\$ 连接，如下图所示。



提示

激活远程注册表服务后，用户就可以通过在“注册表编辑器”窗口中单击“文件”|“连接网络注册表”命令对远程计算机上的注册表项进行修改了。

- 基础知识
- 与嗅探工具
- 系统漏洞攻防
- 安全策略
- 系统与安全
- 系统加密
- 远程控制
- 木马
- 聊天软件
- 网页恶意
- 代码攻防
- 电子邮件
- 病毒
- 使用电脑
- 黑客技巧



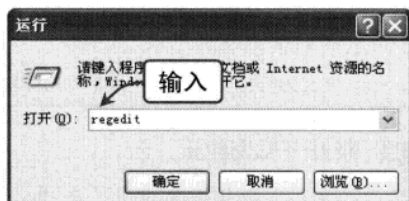
6.2.2 修改注册表实现远程监控

为了方便网络管理员对网络中的计算机进行管理，在 Windows 操作系统的注册表编辑器中设计了“连接网络注册表”功能，管理人员和用户通过注册表可以在网络上检查系统的配置和设置，使得远程管理得以实现。但是该功能却能够被黑客所利用，对他人的注册表进行远程操作。

通过网络连接到注册表的具体操作步骤如下：

STEP 01 打开“运行”对话框

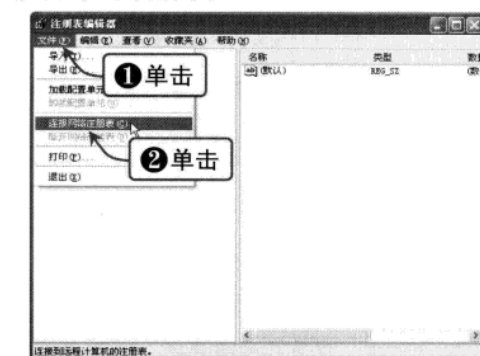
单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令“regedit”，如下图所示。



STEP 02 单击“连接网络注册表”命令

STEP 03 打开“选择计算机”对话框

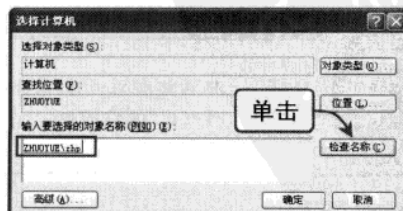
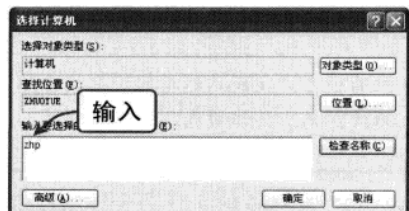
单击“开始”|“运行”命令，打开“运行”对话框，在“打开”下拉列表框中输入命令“regedit”，如下图所示。



打开“选择计算机”对话框，在“输入要选择的对象名称（例如）”文本框中输入希望连接到其注册表的目标主机，如下图所示。

STEP 04 单击“检查名称”按钮

单击“检查名称”按钮，将自动对所填名称进行检测，如存在此目标，则会自动将其名称更改为正确路径，如下图所示。

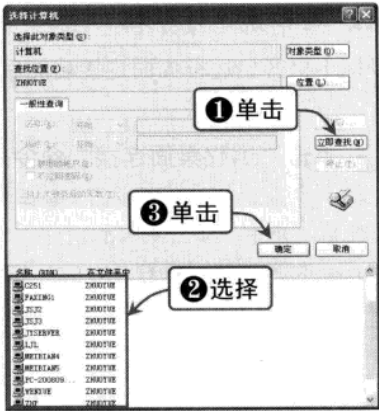


Chapter 06 远程控制攻防

STEP 05 左侧窗格中出现目标主机

用户也可以单击“高级”按钮，启用高级模式，并单击“立即查找”按钮搜索计算机，然后选中想要连接的计算机，单击“确定”按钮将其添加到文本框中，如右图所示。

单击“确定”按钮进行连接，连接成功后，即可在左侧窗格中显示远程计算机的注册表中的相关选项。



6.3 Windows XP 远程控制

远程桌面连接组件从 Windows 2000 Server 开始由微软公司提供，在 Windows 2000 Server 中它不是默认安装的。该组件一经推出受到了很多用户的拥护和喜好，所以在 Windows XP 和 2003 中微软公司将该组件的启用方法进行了改革，用户通过简单的设置就可以完成在 XP 和 2003 下远程桌面连接功能的开启。

6.3.1 Windows XP 系统的远程协助

下面以 Windows XP 为例，详细介绍远程桌面连接的方法。

Work1 开启远程桌面连接

要进行远程协助操作，首先要在目标主机上开启远程桌面连接功能，其具体操作方法如下：

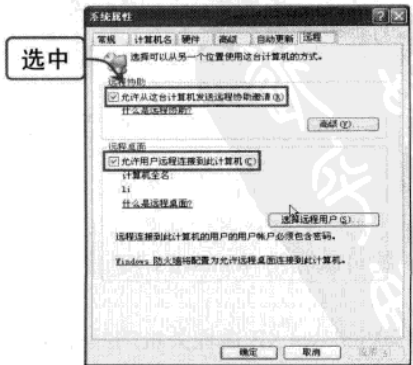
STEP 01 选择“属性”选项

在目标主机桌面的“我的电脑”图标上右击，在弹出的快捷菜单中选择“属性”选项，如下图所示。



STEP 02 开启远程桌面连接功能

弹出“系统属性”对话框，选择“远程”选项卡，然后分别选中“允许从这台计算机发送远程协助邀请”和“允许用户远程连接到此计算机”复选框，单击“确定”按钮，如下图所示。



黑客
常用扫描
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码
攻击防
电子邮
件攻防
二盘病
使用电
脑安全
软件防
黑客攻
防技巧



Work2 远程操作计算机

目标主机开启远程桌面连接功能后，即可通过网络远程登录此计算机，其具体操作方法如下：

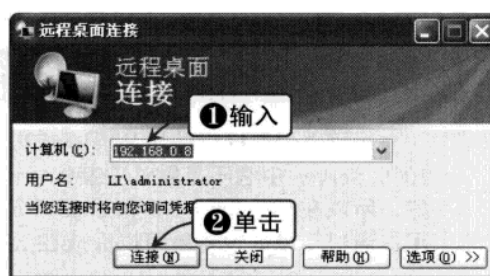
STEP 01 单击“远程桌面连接”命令

单击“开始”|“所有程序”|“附件”|“远程桌面连接”命令，如下图所示。



STEP 02 输入目标主机的 IP 地址

打开“远程桌面连接”窗口，在“计算机”下拉列表框中输入目标主机的 IP 地址，然后单击“连接”按钮，如下图所示。



STEP 03 “登录到 Windows”对话框

弹出“登录到 Windows”对话框，然后在下面的文本框中输入用户名和密码，单击“确定”按钮，如下图所示。



STEP 04 连接到远程主机进行操作

此时即可连接到远程主机，用户可以像操作自己电脑一样对其进行操作，如下图所示。



6.3.2 Windows XP 远程关机

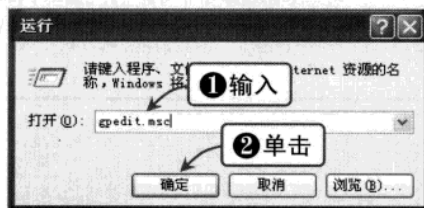
在 Windows XP 默认的安全策略中，只有管理员组的用户才有权从远端关闭计算机，要实现远程关机，必须在客户计算机（能够被远程关闭的计算机）中赋予 guest 用户远程关机的权限，这可以利用 Windows XP 的“组策略”或“管理工具”中的“本地安全策略”来实现。

设置 Windows XP 远程关机的具体操作步骤如下：

Chapter 06 远程控制攻防

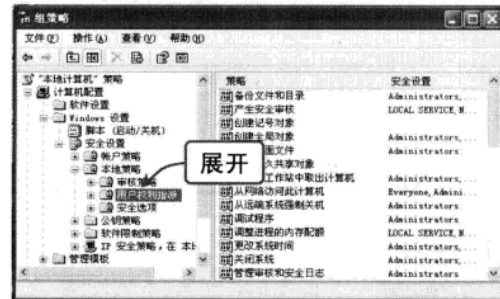
STEP 01 输入 gpedit.msc 命令

单击“开始”|“运行”命令，打开“运行”对话框，然后在文本框中输入 gpedit.msc 命令，单击“确定”按钮，如下图所示。



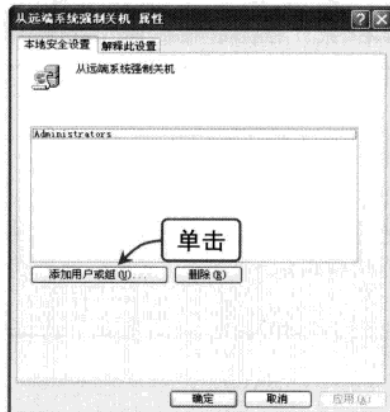
STEP 02 选择“用户权利指派”选项

打开“组策略”窗口，在左侧窗格中依次展开“计算机配置”|“Windows 设置”|“安全设置”|“本地策略”|“用户权利指派”选项，如下图所示。



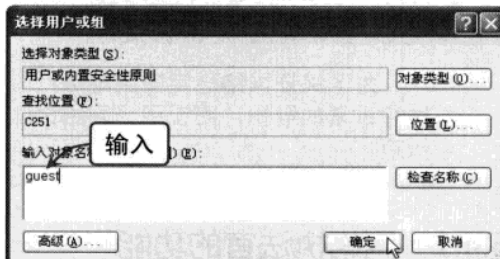
STEP 03 从远端系统强制关机

在“组策略”窗口的右侧窗格中双击“从远端系统强制关机”选项，打开“从远端系统强制关机 属性”对话框，单击该对话框下方的“添加用户或组”按钮，如下图所示。



STEP 04 输入用户名

在弹出的“选择用户或组”对话框中输入 guest，如下图所示。单击“确定”按钮返回“组策略”窗口，关闭该窗口。



提示



单击“确定”按钮返回，在“从远端系统强制关机 属性”对话框中便添加了一个 guest 用户，这样就为 guest 用户授予了远程关机的权限。

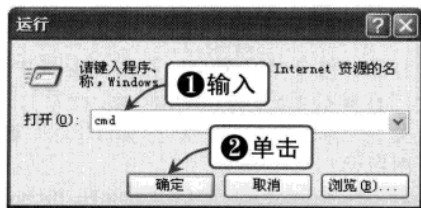
STEP 05 输入 cmd 命令

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 cmd 命令，单击“确定”按钮，如下图所示。

STEP 06 输入远程关机命令

打开“命令提示符”窗口，在其中输入命令“shutdown -s -m \\li -t 30”，如下图所示。

黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
网页恶
代码攻
件攻防
电子邮
C 盘病
使用电
安全软
黑客攻
实用技



提示

这时，在远程计算机的屏幕上将显示一个“系统关机”提示信息框，提示用户“系统即将关机。请保存所有正在运行的工作，然后注销。未保存的改动将会丢失。关机是由 L1NGuest 初始的。”，在该提示信息框下方还有一个计时器，显示离关机还有多少时间，如右图所示。



6.4 使用网络执法官

为了保证网络稳定安全地运行，网络管理人员需要耗费很大精力来对网络进行日常的维护，而使用“网络执法官”这款软件可以轻松解决很多网络安全问题。

6.4.1 网络执法官的功能

网络执法官是一款局域网管理辅助软件，采用网络底层协议，能穿透各客户端防火墙对网络中的每一台主机（本书中主机指各种计算机、交换机等配有 IP 的网络设备）进行监控。该软件采用网卡号（MAC）识别用户，可靠性高；软件本身占用网络资源少，对网络没有不良影响；软件不需运行于指定的服务器，在网内任一台主机上运行即可有效监控所有本机连接到的网络（支持多网段监控）。网络执法官的主要功能如下：

1. 实时记录上线用户并存档备查

网络中任一台主机，开机即会被本软件实时检测并记录其网卡号、所用的 IP、上线时间、下线时间等信息，该信息自动永久保存，可供查询，查询可依各种条件进行，并支持模糊查

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

询。利用此功能，管理员随时可以知道当前或以前任一时刻任一台主机是否开机、开机多长时间，使用的是哪一个 IP、主机名等重要信息或任一台主机的开机历史。

2. 自动侦测未登记主机接入并报警

管理员登记完或软件自动检测到所有合法的主机后，可在软件中做出设定，拒绝所有未登记的主机接入网络。一旦有未登记主机接入，软件会自动将其 MAC、IP、主机名、上下线时段等信息作永久记录，并可采用声音、向指定主机发消息等多种方式报警，还可以根据管理员的设定，自动对该主机采取 IP 冲突、与关键主机隔离、与网络中所有其他主机隔离等控制措施。

3. 限定各主机的 IP, 防止 IP 盗用

管理员可对每台主机指定一个 IP 或一段 IP，当该主机采用超出范围的 IP 时，软件会判定其为“非法用户”，自动采用管理员事先指定的方式对其进行控制，并将其 MAC、IP、主机名做记录备查。管理员可事先指定对非法用户实行 IP 冲突、与关键主机隔离、与其他所有主机隔离等管理方式。

4. 限定各主机的连接时段

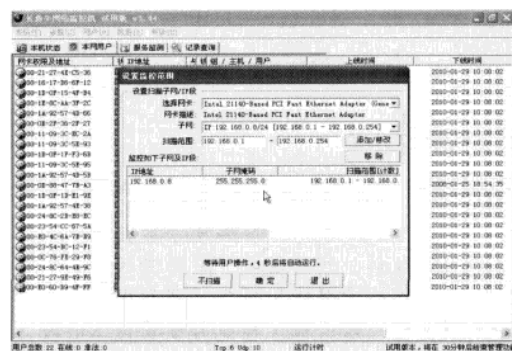
管理员可指定每台主机在每天中允许与网络连接的时段或不允许与网络连接的时段(可指定两个时段,如允许每天 8:30~12:00 和 13:30~17:00 与网络连接),并可指定每一用户是否被允许在每个周六、周日与网络连接。对违反规定的用户,软件判其为非法用户,自动记录并采用管理员事先指定的方式进行管理。管理方式同样可为 IP 冲突、与关键主机隔离、与其他所有主机隔离等。

6.4.2 认识网络执法官的操作界面

在使用网络执法官之前，首先要对其操作界面进行了解。

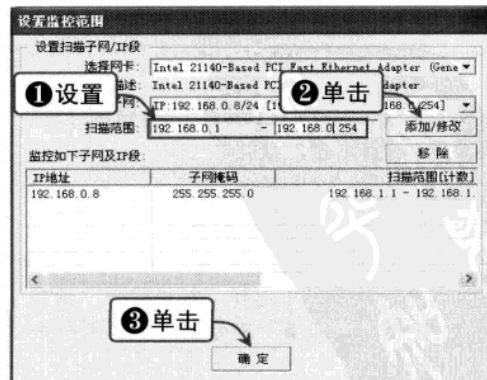
STEP 01 打开网络执法官

下载并安装网络执法官后，双击其程序图标，打开其开始界面，并弹出“设置监控范围”对话框，如下图所示。



STEP 02 设置扫描范围

在“扫描范围”右侧的文本框中设置局域网 IP 地址的范围,然后单击“添加/修改”按钮,将此范围添加到下面的列表框中,如下图所示。单击“确定”按钮返回主界面。

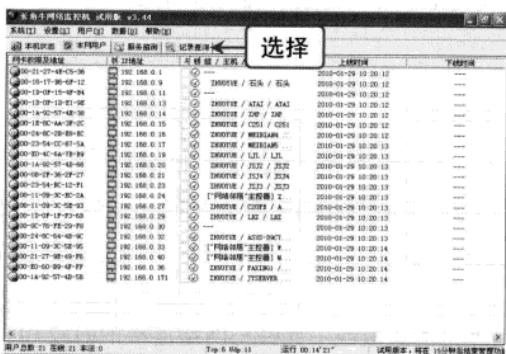


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



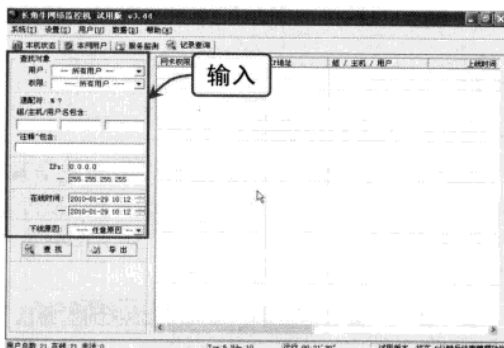
STEP 03 显示本网用户信息

此时，即可看到“本网用户”选项卡中详细列出了局域网内所有计算机的信息，包括网卡权限及地址、状态、IP 地址、与本机流量、是否锁定、域/主机/用户、上线和下线时间及网卡注释等，如下图所示。



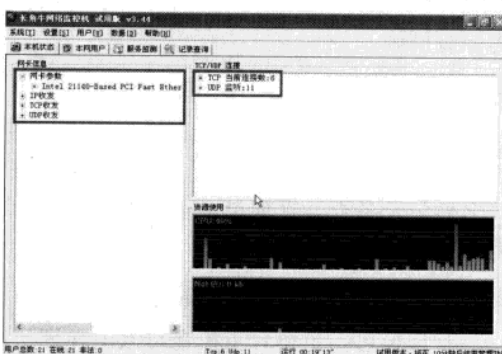
STEP 05 记录查询

选择“记录查询”选项卡，可以查看系统所记录的所有上线用户的信息，用户可以输入各种条件查询并统计，如下图所示。



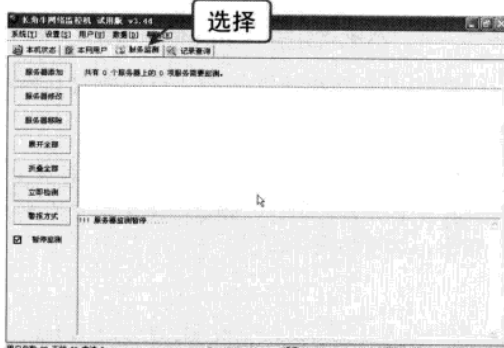
STEP 04 显示本机状态

选择“本机状态”选项卡，在左侧窗格中列出了网卡参数、IP 收发、TCP 收发以及 UDP 收发等信息，右上方窗格中列出了 TCP/UDP 连接数，右下方窗格中以图表形式列出了 CPU 的资源利用率和网络数据传输量，如下图所示。



STEP 06 服务监测

选择“服务监测”选项卡，可以对局域网中的服务器进行监测，保障网络服务器的安全，如下图所示。



6.4.3 网络执法官的常用操作

下面根据网络执法官的各项功能，对其常用操作进行介绍。

STEP 01 打开“用户权限设置”对话框

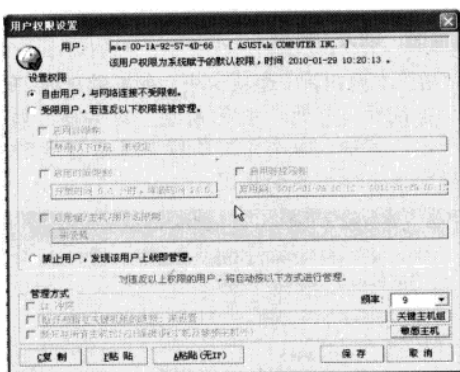
在“本网用户”选项卡的目标主机上右击，在弹出的快捷菜单中选择“权限设置”选项，弹出“用户权限设置”对话框，如下图所示。

STEP 02 “每日时段权限设置”对话框

选中“受限用户，若违反以下权限将被管理”单选按钮，然后选中“启用时间限制”复选框，并单击被激活的选项，将弹出“每日时段权限设置”对话框，在此可设置具体时段，如下图所示。

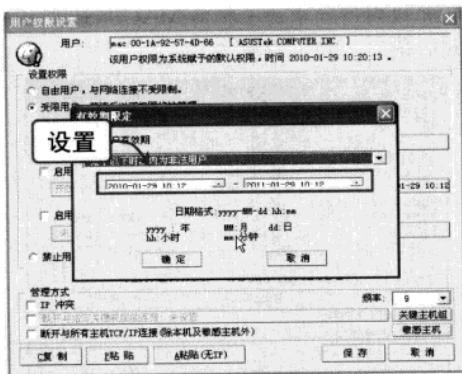
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 06 远程控制攻防



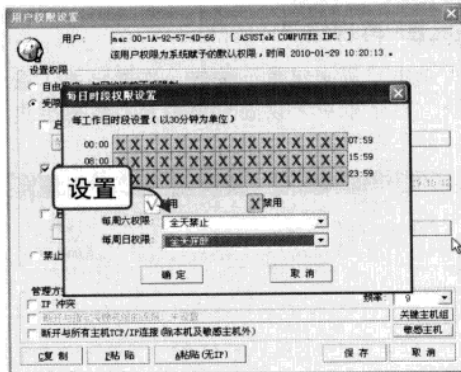
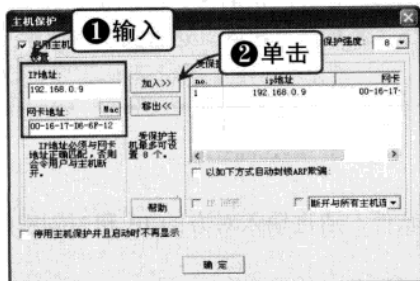
STEP 03 “有效期限定”对话框

如果在“用户权限设置”对话框中选中“启用时段限制”复选框，然后单击下面被激活的选项，将弹出“有效期限定”对话框，在此可以设置具体的起始时间，如下图所示。



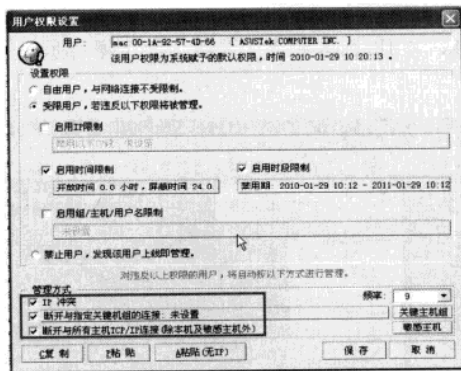
STEP 05 添加受保护的主机

单击“设置”|“主机保护”命令，弹出“主机保护”对话框，在该对话框中选中“启用主机保护”复选框，然后在下面的文本框中输入IP地址和网卡地址，并单击“加入”按钮，将其添加到右侧的列表框中，如下图所示。



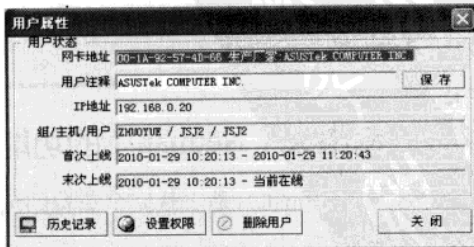
STEP 04 设置管理方式

在“用户权限设置”对话框下方的“管理方式”选项区中可以选择对违反上述权限的用户怎样处理，在此有三种方式：IP冲突、断开与指定关键机组的连接和断开与所有主机TCP/IP连接，如下图所示。



STEP 06 打开“用户属性”对话框

在“本网用户”选项卡的目标主机上右击，在弹出的对话框中选择“属性”选项，弹出“用户属性”对话框，如下图所示。



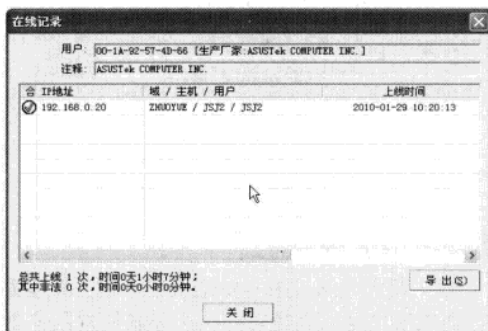
基础
知识
与
工
具
黑
客
常
用
扫
描
工
具
统
漏
洞
攻
防
安
全
策
略
系
统
与
文
件
加
密
远
程
控
制
攻
防
木
马
防
御
件
攻
防
网
页
恶
意
代
码
攻
防
电
子
邮
件
攻
防
C
盘
病
毒
攻
防
安
全
软
件
使
用
电
脑
黑
客
攻
防
实
用
技
巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



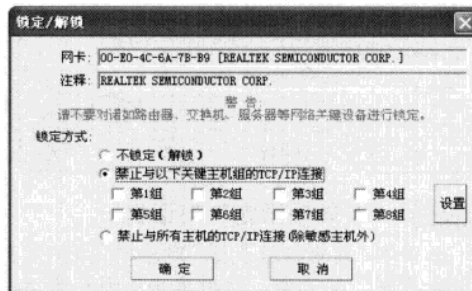
STEP 07 再现记录

单击“历史记录”按钮，在弹出的“在线记录”对话框中可以查看该用户在线的历史记录，如下图所示。



STEP 08 锁定/解锁

在“本网用户”选项卡中，在某用户的“锁”列双击鼠标，打开“锁定/解锁”对话框，如下图所示。其中，每个用户的锁定状态有 3 种：未锁定、半锁定和全锁定。



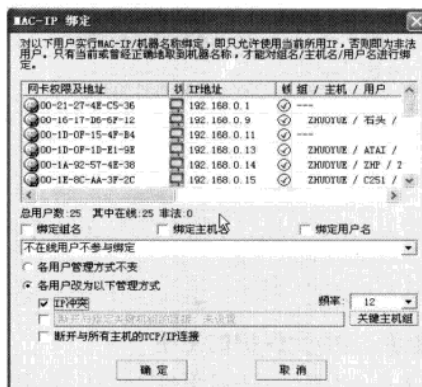
STEP 09 选择“绑定 MAC 与 IP”选项

在“本网用户”选项卡中将所有用户选中，然后右击，在弹出的快捷菜单中选择“绑定 MAC 与 IP/机器名称”选项，如下图所示。



STEP 10 “MAC-IP 绑定”对话框

弹出“MAC-IP 绑定”对话框，在该对话框中可以对所选中的主机的 MAC 地址与 IP 地址进行绑定，如下图所示。



6.5 使用远程控制软件

通过网络我们可以在城市的一边使用计算机控制另外一边的计算机，从而不用花费大量精力亲自到机房操作服务器。如何操作远程的计算机呢？这就要使用远程控制软件。

6.5.1 网络人 (Netman) 的功能

网络人 (Netman) 是一款完全免费的远程控制软件，通过输入对方的 IP 和控制密码就能实现远程监控。

Chapter 06 远程控制攻防

软件使用 UDP 协议穿透内网，不用做端口映射用户就能在任何一台可以上网的电脑连接远端电脑，进行远程办公和远程管理。它是正规合法的软件，不会被杀毒软件当做病毒查杀，不会影响系统的稳定性。

网络人的主要功能包括以下几点：

- ❖ 实现隐蔽监控：隐藏被控端网络人程序图标及相关提示，被控时不被发觉。
- ❖ 远程访问桌面：同步查看远程电脑的屏幕，能使用本地鼠标键盘如操作本机一样操作远程电脑。
- ❖ 可对远程电脑屏幕进行拍照或录像，控制端只需点击功能键便可以切换双方身份，应用于远程电脑维护、远程技术支持和远程协助等。
- ❖ 远程文件管理：上传、下载文件，远程修改、运行文件，实现连接双方电脑的资源共享，用于远程办公等。
- ❖ 远程开启视频：开启远端电脑摄像头，进行语音视频聊天。支持视频录制，可远程旋转带有旋转功能的摄像头，用于家庭安全监控等。
- ❖ 远程命令控制：远程开机（需配合使用网络人电脑控制器硬件）、远程关机、远程重启、远程注销、锁定本地或远端电脑的鼠标键盘等。

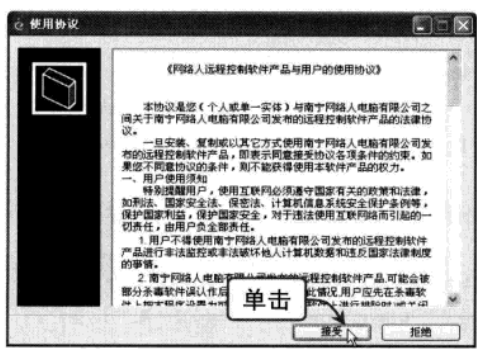
6.5.2 网络人 (Netman) 的使用

网络人分为远程办公版和远程监控版，一台电脑只能安装一个版本，如果安装错了，可在安装目录中运行卸载程序并重启电脑后再安装另外一个版本。

使用网络人的具体操作方法如下：

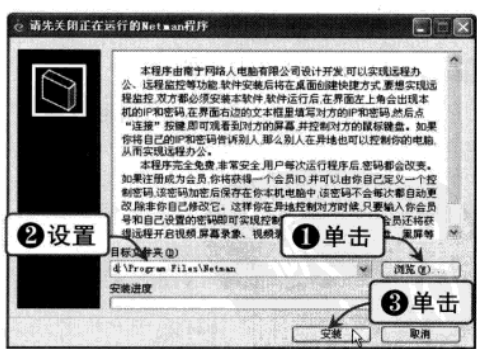
STEP 01 打开“使用协议”窗口

运行网络人办公版安装程序图标，在打开的“使用协议”窗口中单击“接受”按钮，如下图所示。



STEP 02 设置软件安装目录

在弹出的窗口中单击“浏览”按钮设置软件安装目录，然后单击“安装”按钮开始安装，如下图所示。



STEP 03 “记事本”窗口

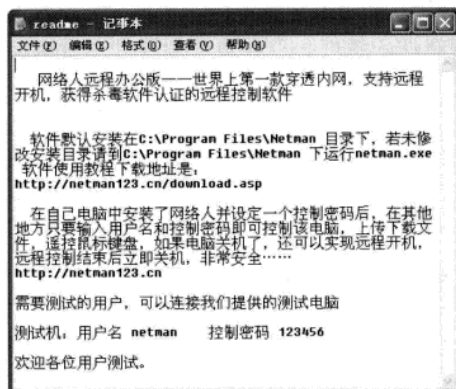
软件安装完毕后，将弹出一个“记事本”窗口，提醒用户安装完毕，并给出测试机的地址，如下图所示。

STEP 04 “使用协议”窗口

在要控制的计算机上运行网络人远程监控版安装程序图标，在打开的“使用协议”窗口中单击“接受”按钮，如下图所示。

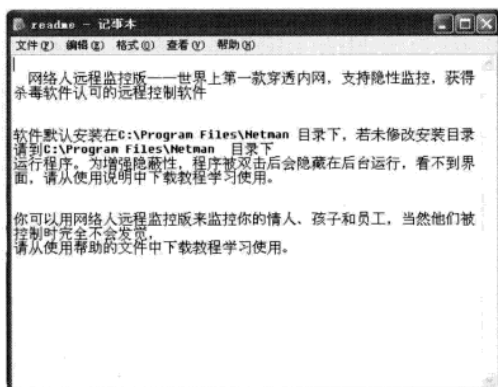
- 基础知 黑客
- 常用扫描 与嗅探工具
- Windows 系统漏洞攻防
- 设置系统 安全策略
- 系统与文 件加密
- 远程控 制攻防
- 木马 攻防
- 聊天软 件攻防
- 网页恶 意代码攻 防
- 电子邮 件攻防
- C 盘病 毒攻防
- 使用电 脑安全软 件
- 黑客攻 防实用技 巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



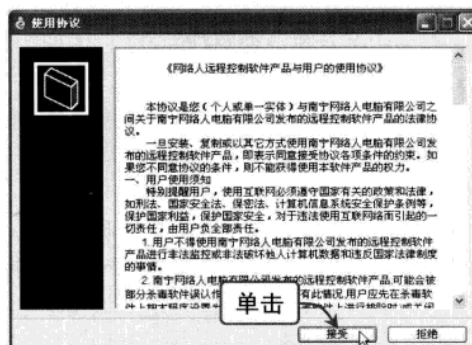
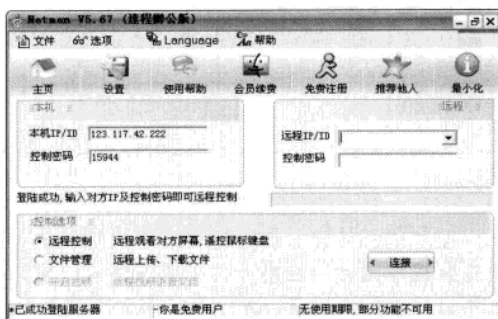
STEP 05 打开“记事本”窗口

在弹出的对话框中设置软件安装路径，然后单击“安装”按钮开始安装，安装完毕后将弹出如下图所示的“记事本”窗口。



STEP 07 打开主控机主界面

在主机上单击“开始”|“所有程序”| Netman |“网络人”命令，打开程序主界面，如下图所示。



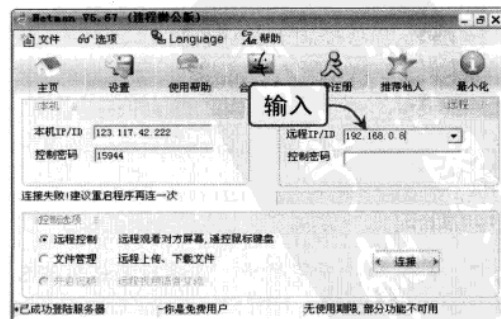
STEP 06 运行监控端程序

找到监控程序的安装路径，然后双击监控程序图标，运行监控端程序，此程序将在后台隐藏运行，如下图所示。



STEP 08 输入监控机的 IP 地址

在“远程 IP/ID”右侧的下拉列表框中输入监控机的 IP 地址（在此以 192.168.0.0 为例），如下图所示。

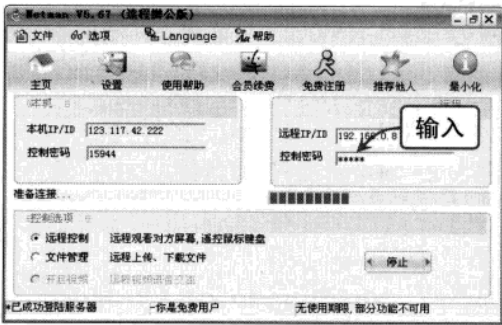


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 06 远程控制攻防

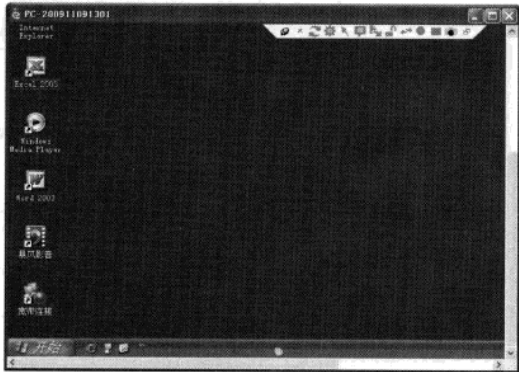
STEP 09 开始连接远端主机

在“控制密码”文本框中输入密码，然后单击“连接”按钮，开始连接远端主机，如下图所示。



STEP 10 弹出提示信息框

稍后即可显示远程主机控制界面，用户现在就可以对远程主机进行操作了，如下图所示。



● 读书笔记

Blank lined area for reading notes.

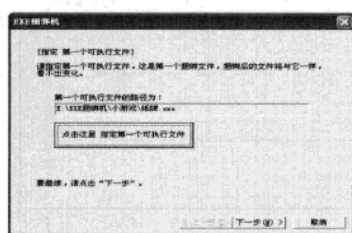
- 黑客
- 基础知识
- 常用扫描与嗅探工具
- Windows系统漏洞攻防
- 设置系统安全策略
- 系统与文件加密
- 远程操控攻防
- 木马攻防
- 聊天软件攻防
- 网页恶意代码攻防
- 电子邮箱攻防
- C盘病毒攻防
- 使用电脑安全软件
- 黑客攻防实用技巧

Chapter

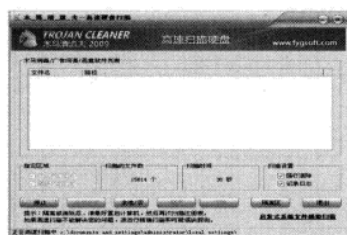
07

木马攻防

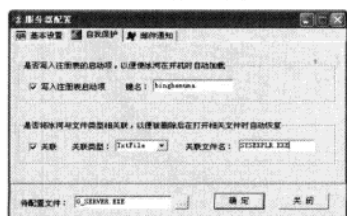
木马程序是目前比较流行的病毒程序，它是一种基于远程控制的黑客工具。由于木马技术具有隐蔽性、自发性和非授权性等特点，已经成为黑客们常用的攻击手段。本章从木马的特性和原理入手，讲解木马程序的制作以及如何全面防范木马攻击。



指定第一个捆绑文件



高速硬盘扫描



自我保护

重要知识点视频索引



本章建议学习时间：

本章建议学习时间为 60 分钟，其中分配 10 分钟学习木马基础知识，15 分钟学习木马的制作方法，15 分钟学习木马的清除与防范，10 分钟学习“冰河”木马的使用与清除方法，10 分钟学习“广外女生”木马的使用与清除方法。

学完本章后您可以：

- 了解木马基本知识
- 了解木马特性与原理
- 常见木马制作和防范
- 一般木马的清除方法
- “冰河”木马的使用与清除
- “广外女生”木马的使用与清除

7.1 木马基础知识

木马（Trojan），也叫特洛伊木马，这个名字最早起源于古希腊传说中的木马计的故事。在计算机领域，木马特指一类恶意程序。由于木马技术具有隐蔽性、自发性和非授权性等特点，因此成为黑客们常用的攻击手段。

7.1.1 木马的概念和结构

“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，但是通过它可以对电脑系统进行强有力的远程控制、窃取密码、控制系统操作和文件操作等破坏性操作。

从木马的发展来看，基本上可以分为以下五个发展阶段：

第一代木马在网络还处于以 UNIX 平台为主的时期就产生了。而针对 Windows 系统的第一代木马为数不多，只有 BO、Netspy 等少量木马，功能也非常简单。Windows 木马只是一个将自己伪装成特殊的程序或文件的软件，如将本身伪装成一个用户登录窗口，当用户运行了木马伪装的登录窗口，输入用户名与密码后，木马将自动记录数据并转发给入侵者，入侵者借此来获得用户的重要信息，达到自己的目的。

第二代木马相对于第一代木马，技术与功能出现了质的变化。随着 Windows 平台的日益普及，一些基于图形操作的木马程序出现了，用户界面的改善使使用者不用懂太多的专业知识就可以熟练地操作木马，木马入侵事件也频繁出现。而且由于这个时期木马的功能已日趋完善，提供了几乎所有能够进行的远程控制操作，因此对服务端的破坏也更大了。

第三代木马继续完善了连接与文件传输技术，增加了木马穿透防火墙的功能，并出现了“反弹端口”技术，如国内的灰鸽子木马软件。

第四代木马除了完善之前所有的技术外，还利用了远程线程插入技术，将木马线程插入 DLL 线程中，使系统更加难以发现木马的存在与入侵的连接方式。

第五代木马相对于第四代木马，功能更加全面，而且应用动态链接库技术（DLL 技术）后在目标主机的计算机中不生成新的文件。而且某些第五代木马已经可以嵌入任何线程中，这使得木马更加隐蔽。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。

1. 硬件部分：建立木马连接所必需的硬件实体

控制端：对服务端进行远程控制的一方。

服务端：被控制端远程控制的一方。

Internet：控制端对服务端进行远程控制，数据传输的网络载体。

2. 软件部分：实现远程控制所必需的软件程序

控制端程序：控制端用以远程控制服务端的程序。

木马程序：潜入服务端内部，获取其操作权限的程序。运行了木马程序以后，被攻击者的电脑就会有一个或几个端口被打开，使黑客可以利用这些打开的端口进入电脑系统，安全和个人隐私也就全无保障了。木马的设计者为了防止木马被发现，而采用多种手段隐藏木马。

基础知
识

常用扫
描工
具

统漏
洞防
攻

安全策
略

系统
与文
件加
密

远程
控
制

攻
防

件攻
防

代
码
攻
防

件
攻
防

毒
攻
防

安
全
软
件

黑
客
攻
防



木马的服务一旦运行并被控制端连接，其控制端将享有服务端的大部分操作权限，例如给计算机增加口令，浏览、移动、复制、删除文件，修改注册表，更改计算机配置等。

木马配置程序：设置木马程序的端口、触发条件、木马名称等，使其在服务端藏得更隐蔽。

3. 连接部分：通过 Internet 在服务端和控制端之间建立一条木马通道

控制端 IP，服务端 IP：即控制端、服务端的网络地址，也是木马进行数据传输的目的地。

控制端端口，木马端口：即控制端、服务端的数据入口，通过这些入口数据可直达控制端程序或木马程序。

7.1.2 木马的分类

自木马程序诞生至今，已经出现了多种类型，大多数的木马都不是单一功能的木马，它们往往是很多种功能的集成品。根据黑客攻击目的的不同，主要分为以下几类：

1. 破坏型

唯一的的功能就是破坏并且删除文件，可以自动删除电脑上的 DLL、INI、EXE 文件。

2. 密码发送型

这种木马可以找到隐藏密码记录，并把获取的密码发送到指定的信箱。

有部分用户喜欢把自己的各种密码以文件的形式存放在计算机中备忘，认为这样方便；或者用 Windows 提供的密码记忆功能，这样就可以不必每次都输入密码了。这些看似方便的操作，实际为木马软件的扫描打开了方便之门。

3. 远程访问型

远程访问型木马程序一般包括客户端程序和服务端程序，在目标主机上执行了服务端程序后，只要用户知道目标主机的 IP 地址或主机名，就可以与目标主机连接。连接成功后，用户通过客户端程序提供的远程操作功能就可以实现对目标主机的监视与控制。

利用这类木马的目的取决于用户，此类程序完全可以用于医院或学校等正当领域。例如，在上机试验课中，老师可以通过远程访问程序来对学生的电脑进行监控，以确定学生正在进行课上应该完成的实验，而不是聊天或游戏。

此类木马程序中采用的是 UDP 协议（user datagram protocol，用户报文协议），此协议是因特网上广泛采用的通信协议之一。与 TCP 协议不同，它是一种非连接的传输协议，没有确认机制，可靠性不如 TCP，但它的效率却比 TCP 高，用于远程屏幕监视还是比较适合的。远程访问型木马程序不区分服务器端和客户端，只区分发送端和接收端，编程上较为简单，因此选用 UDP 协议。

4. 键盘记录型

顾名思义，这类木马程序的主要功能就是记录用户的键盘操作。它们一般是随着 Windows 的启动而启动，并且可以分别记录在线状态和离线状态下的键盘操作，从而盗取用户的账号、密码，甚至安全证书等信息。

5. DOS 攻击型

随着 DOS 攻击越来越广泛被应用，被用做 DOS 攻击的木马也越来越流行起来。当入侵者入侵了一台机器后，给目标主机种上 DOS 攻击木马，那么日后这台计算机就成为入侵者进行 DOS 攻击的最得力助手了，即所谓的“肉鸡”。入侵者控制的“肉鸡”数量越多，发动 DOS 攻击取得成功的概率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在可以攻击多台计算机，以致给网络造成很大的伤害和损失。

还有一种类似 DOS 的木马叫做邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪、不能接收邮件为止。

6. 代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用 Telnet、QQ、IRC 等程序，从而隐藏自己的踪迹。

7. FTP 木马

这种木马可能是最简单和古老的木马了，它的唯一功能就是打开 21 端口，等待用户连接。现在新 FTP 木马还加上了密码功能，这样只有攻击者本人才知道正确的密码，从而进入对方计算机。

8. 程序杀手木马

现在用户的计算机一般都装载了防木马的软件，如瑞星防火墙、ZoneAlarm、Norton 等。要想让以上各类木马完全发挥自己的功用，就必须要通过防木马软件的阻拦。程序杀手木马就是这类软件，它的作用就是关闭被攻击方计算机上运行的防木马软件、防火墙等，为随后而来的木马军团打开方便之门。

9. 反弹端口型木马

木马开发者在分析了防火墙的特性后发现：防火墙对于连入的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马在服务端使用主动端口，客户端使用被动端口。木马定时监测客户端的存在，发现客户端上线立即进行主动连接；为了隐蔽起见，客户端的被动端口一般为 80，即使用户使用扫描软件检查自己的端口，也不会发现什么异常的数据包，这样就会以为是在正常浏览网页。

7.1.3 木马的特点

随着计算机技术的迅速发展，木马病毒的种类和数量也层出不穷，综合目前流行的木马病毒，可归纳为具有以下几个特点：

1. 隐蔽性

木马的隐蔽性是其首要特征。如其他所有的病毒一样，木马也是一种病毒，它必须隐藏在用户的系统之中，它会想尽一切办法藏匿自己的运行活动而不被发现。例如，大家所熟悉的木马修改注册表和 ini 文件以便机器在下次启动后仍能载入木马程式，它不是自己生成



一个启动程序，而是依附在其他程序之中。有些把服务器端和正常程序绑定成一个程序的软件，叫做 exe-binder 绑定程序，可以让人在使用绑定的程序时，木马也入侵了系统，甚至有个别木马程序能把它自身的 exe 文件和服务器端的图片文件绑定，在你看图片的时候，木马也侵入了你的系统。还有些木马把自己注册为系统服务，并设置服务属性为“自动”。由于所有属性为“自动”的服务都会在开机时被执行，木马也就会随之以正常服务状态运行，而不被用户发现。

2. 潜伏性

木马能够和已经被捆绑的程序一起等待该程序被运行才启动该木马，从而毫无声息地打开端口等待外部连接。

3. 自动运行性

它是一个当用户系统启动时即自动运行的程序，所以它必须潜入用户计算机的启动配置文件中，运行并加载到系统自启动程序序列中，如 win.ini、system.ini、winstart.bat 以及启动组等文件之中。

4. 欺骗性

木马程序要达到其长期隐蔽的目的，就必须借助系统中已有的文件，以防被用户发现。它经常使用的是常见的文件名或扩展名，如 dll\win\sys\explorer 等字样，或者仿制一些不易被人区别的文件名，如字母 l 与数字 1、字母 o 与数字 0，常修改基本文件中的这些难以分辨的字符，更有甚者干脆就借用系统文件中已有的文件名，只不过它保存在不同路径之中。还有的木马程序为了隐藏自己，常把自己设置成一个 ZIP 文件式图标，当用户一不小心打开它时就马上运行。

5. 自动恢复性

现在很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。

6. 自动打开特别端口

木马程序潜入用户的计算机之中的目的主要不是为了破坏系统，更是为了获取用户系统中有用的信息，这样用户上网时能与远端服务器进行通信，木马程序就会用服务器/客户端的通信手段把信息告诉黑客们，以便黑客们控制用户的机器，或实施更进一步的入侵企图。

7. 通用性

不受客户端操作系统和服务配置限制。即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

7.1.4 木马的入侵和启动

目前木马入侵的主要途径还是先通过一定的方法让木马执行文件进驻到被攻击者的计算机系统里，如邮件、下载等，然后通过一定的提示故意误导被攻击者打开执行文件。一般的木马执行文件非常小，大多是几 KB 到几十 KB，如果把木马捆绑到其他正常文件中，用户也是很难发现的。此外，木马也可能通过 Script、ActiveX 及 Asp.CGI 等交互脚本进行传

播。利用这些途径进驻了被攻击者的计算机后，木马就开始通过各种方式启动木马程序入侵我们的计算机了。

Work1 木马入侵方式

目前木马入侵的主要途径还是先通过一定的方法让木马执行文件进驻到被攻击者的计算机系统中里。木马入侵方式主要有以下几种：

1. 利用系统漏洞

攻击者最常使用的攻击手法就是扫描寻找系统漏洞，利用系统的安全漏洞实施木马种植。攻击者通常会把木马发布在一个吸引人的网站上，比如免费聊天室、免费电影下载站等，存在系统漏洞的电脑浏览这些网站就会自动下载并执行木马。

2. 会话劫持攻击

正常上网时，客户端和远程的服务器之间会建立会话，客户端软件（利用 IE 浏览器）把服务器提供的内容下载到本地。木马攻击者此时会利用 ARP 欺骗或其他方式，劫持客户端和服务端的会话，把一个经过篡改的信息返回给客户端，客户端就会下载攻击者指定的恶意代码。利用会话劫持可以迅速将挂马的战果放大，是黑客最喜欢的攻击手段。因为大量发送 ARP 攻击包对局域网影响很大，客户机经常会断网，网速也会因此变慢，给网络管理带来极大挑战。局域网用户遭遇会话劫持后，会发现多台客户机访问很多站点时，杀毒软件提示发现木马 ARP 攻击包效果。

3. QQ、电子邮件冒名欺骗

攻击者盗取了某个 QQ 号，然后立即和该 QQ 号的好友联系，尝试发送木马。接收者往往以为是自己信任的朋友，会降低警惕，从而运行木马程序。或者用匿名邮件冒充好友或知名企业、机构向对方发木马附件，诱骗其下载并运行附件。

4. 危险下载点

攻破一些下载站或者自己提供几个热门工具下载，在程序中捆绑木马。

Work2 木马启动方式

木马利用以上途径进驻了被攻击者的计算机后，就开始通过以下几种主要方式启动木马程序，入侵用户的计算机系统。

1. 在 win.ini 文件中加载

在 win.ini 的 [Windows] 字段中有启动命令“load=”和“run=”。这两项分别是用来当系统启动时自动加载和运行程序的，默认情况下“=”的后面是空白的。如果木马程序加载到这两个子项中，那么当用户的系统启动后木马即可自动运行或加载了。开机加载程序的路径如下：

run=C:\Windows\sample.exe
load=C:\Windows\sample.exe

2. 在*.ini 文件中加载

在应用程序的启动配置文件中，控制端利用这些文件能启动程序的特点，将制作好的



带有木马启动命令的同名文件上传到服务端覆盖这同名文件，这样就可以达到启动木马的目的了。

3. 修改文件关联

修改文件关联是木马常用的手段，例如，在正常情况下某文件的打开方式为 Notepad.EXE，一旦中了文件关联木马，则 TXT 文件打开方式就会被修改为用木马程序打开，如著名的国产木马冰河就是这样。

4. 通过启动组实现自启动

启动组是专门用来实现应用程序自启动的地方。启动组文件夹的位置为 C:\Documents and Settings\Administrator\Start Menu\Programs\Startup。此处 Administrator 为主机的用户名。木马文件如果进入自启动序列中，就可以随着系统的启动而悄无声息地启动了。

5. 修改注册表

木马通过增加注册表中的某几个键值来运行自身，如 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\下的几个以 Run 和 RunServices 开头的键值，在其中可能存在启动木马的键值。

7.1.5 木马的伪装手段

通过前面的介绍，相信读者对于木马已经有了一定的了解，这会对木马的传播起到一定的抑制作用。这是木马设计者所不愿见到的，因此他们开发了多种功能来伪装木马，以达到降低用户警觉、欺骗用户的目的。常用伪装手段有以下几种：

1. 图标伪装

在 Windows 系统中，每种文件类型使用不同的图标进行表示，用户通过一种图标就可以轻易地判断出这是哪种文件类型。黑客为了迷惑用户，将木马服务端程序的图标换成一些常见的文件类型的图标，这样当用户运行它以后木马软件就开始工作了。

2. 名称伪装

图标修改往往和文件改名是一起进行的，黑客往往将文件的名称取得非常诱人，诱骗用户去运行它。当木马服务端程序运行以后，服务端程序也会将自己的进程设置为和正常的系统进程相似的名称，从而使用户不容易产生怀疑，被其麻痹。

3. 捆绑文件

这种伪装手段通常是木马捆绑到一个安装程序上，由于被捆绑的文件一般是可执行文件（即 EXE、COM 一类的文件），所以具有很大的迷惑性。当安装程序运行时，木马就在用户毫无察觉的情况下，偷偷地进入了系统。

4. 出错提示

绝大多数木马服务端安装时不会出现任何图形界面，因此如果一个程序双击后没有任何反应，有经验的用户就会怀疑它是木马。木马的设计者也意识到了这个缺陷，会故意让木马在被运行时弹出一个错误提示对话框，例如“文件已损坏，无法打开”等。如今的木马程序很多都有“安装完毕后显示提示”的选项，例如冰河木马，配置服务端程序后，在“提示内

Chapter 07 木马攻防

容”输入框中输入需要的提示内容。当用户运行服务端程序后，就会弹出所设置的内容。

5. 定制端口

很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马。但是，现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1024~65535 之间任选一个端口作为木马端口（一般不选 1024 以下的端口），这样就给判断所感染木马的类型带来了麻烦。

6. 自我销毁

大多数木马本身只有一个文件，它的安装程序其实就是木马服务端程序，当用户双击了一个木马的安装程序后，它会把自己复制到系统目录或其他目录，因此一些有经验的用户如果怀疑一个程序是木马，它会根据安装程序的大小和修改时间在硬盘上搜索木马文件。为了对付这种勘察方法，一些木马设计了自我销毁的功能，当它把自己复制到系统目录或其他目录后，会把自己删除，让用户无据可查。

7. 伪装成应用程序扩展组件

此类属于最难识别的木马，也是骗术最高的木马。木马编写者用自己编制的特洛伊 dll 替换已知的系统 dll，并对所有的函数调用进行过滤，对于正常的调用，使用函数转发器直接转发给被替换的系统 dll，对于一些事先约定好的特殊情况，dll 会执行一些相对应的操作，一个比较简单的方法是启动一个进程，虽然所有的操作都在 dll 中完成会更加隐蔽，但是这大大增加了程序编写的难度。实际上这样的木马大多数只是使用 dll 进行监听，一旦发现控制端的连接请求就激活自身，启动一个捆绑端口的进程进行正常的木马操作。操作结束后关掉进程，继续进入休眠状况。目前，有些木马就是采用这种内核插入式的嵌入方式，利用远程插入线程技术，嵌入 dll 线程，或者挂接 PSAPI，实现木马程序的隐藏，甚至在 Windows NT/2000/XP 下，都达到了很高的隐藏效果。

8. 网页伪装

黑客成功利用了系统以及一些程序的漏洞后，诱骗用户浏览某个特殊的网页，在用户浏览的时候，网页木马就会成功地利用系统的漏洞，从而将设置的木马服务端程序“悄悄地”安装到远程系统中。

9. 邮件附件

通过电子邮件的附件进行简单的文件传输，本来是为了方便用户，可黑客正是看中了这一点，通过伪造一些著名的企业或用户好友的邮件来欺骗用户，通过邮件附件来传播木马服务端程序。黑客在邮件附件中加入木马后，一般会使用比较有迷惑性的语句来骗取用户的信任。比如“这是 Windows 最新的安全补丁程序，请运行后重新启动系统”，从而达到诱骗用户下载并安装的目的。

7.2 木马的制作

随着计算机技术的日臻成熟，木马的制作方式也相应增多，下面将着重介绍几种常见的木马制作方法以及相应的防范对策。

基础
知识

常用
扫描
与嗅探
工具

Windows
系统
漏洞攻防

设置系统
安全策略

系统与文
件加密

远程控
制攻防

木马
攻防

聊天软
件攻防

网页恶意
代码攻防

电子邮
件攻防

病毒防
毒攻防

使用电脑
安全软件

黑客攻
防技巧



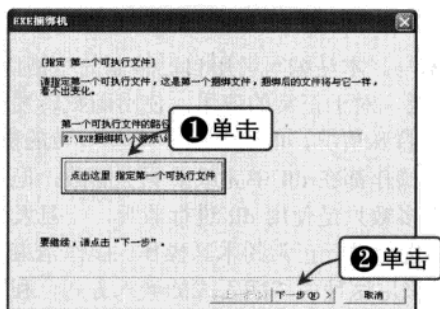
7.2.1 使用“EXE 捆绑机”捆绑木马

一般的木马要进行伪装就必须把自己隐藏在别的文件中，常见的有各种各样的捆绑器。下面以 EXE 捆绑机为例，介绍这类软件的使用方法。

EXE 捆绑机可以把两个可执行程序捆绑成一个程序，执行捆绑后的程序就等于同时执行了两个程序。而且它会自动更改图标，使捆绑后的程序和捆绑前的程序图标一样，做到天衣无缝。可以把木马和其他软件捆绑起来，木马同时悄悄地运行。假设提前做好了木马样本，起名为“木马.exe”，正常程序为“纸牌.exe”。

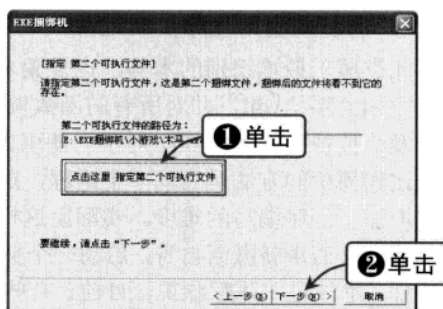
STEP 01 指定第一个捆绑文件

运行 EXE 捆绑机程序后，在弹出的对话框中单击“点击这里指定第一个可执行文件”按钮选定第一个可执行文件（即正常程序文件），单击“下一步”按钮，如下图所示。



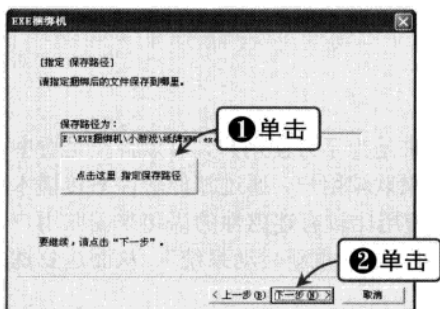
STEP 02 指定第二个捆绑文件

在弹出的对话框中单击“点击这里指定第二个可执行文件”（即要被加载的木马文件）按钮选定第二个可执行文件，单击“下一步”按钮，如下图所示。



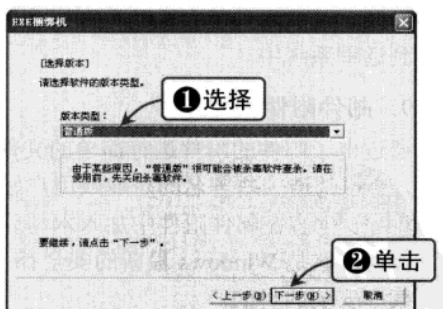
STEP 03 保存文件

单击“点击这里指定保存路径”按钮，指定已经绑定好的文件的保存路径，单击“下一步”按钮，如下图所示。



STEP 04 选择版本类型

在“版本类型”下拉列表框中选择“普通版”选项，并暂时关闭杀毒软件，单击“下一步”按钮，如下图所示。

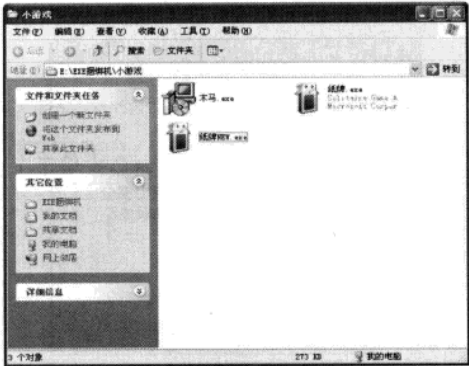
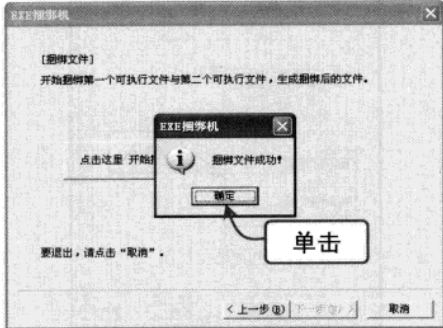


STEP 05 捆绑文件成功

依次单击“下一步”按钮，单击“确定”按钮完成捆绑，如下图所示。

STEP 06 生成新的文件

捆绑成功后，生成一个新的可执行文件，其图标和第一个执行文件名称一样，当运行新的执行文件时，相当于同时运行两个文件，如下图所示。



7.2.2 自解压木马

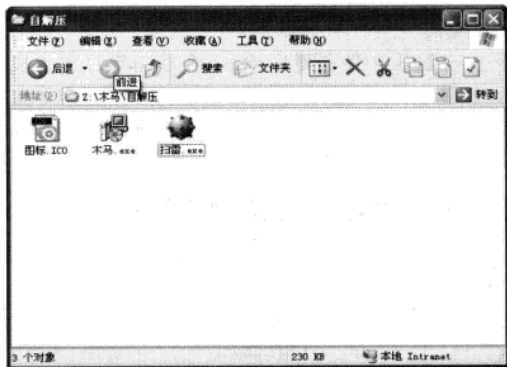
下面将介绍自解压木马的制作与查杀方法。

Work1 自解压木马的制作

利用 WinRAR 的自解压功能不仅可以用来加载隐蔽的木马服务端程序，还可以用来修改对方的注册表。用户所看到的仅是一个可执行文件，而且双击打开后，可能是一个正常的应用程序，但是和该正常的程序压缩在一起的木马程序，则在后台开始运行。具体制作方法如下：

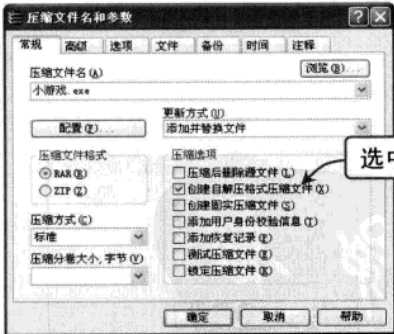
STEP 01 准备压缩

在制作自解压木马前应先准备木马程序、伪装程序、图标文件，并安装 WinRAR 软件，如下图所示。



STEP 02 创建自解压文件

同时选中木马程序和伪装程序并右击，在弹出的快捷菜单中选择“添加到压缩文件”选项。在“压缩文件名和参数”对话框中，选择“常规”选项卡，输入压缩文件的名称，选中“创建自解压格式压缩文件”复选框，如下图所示。



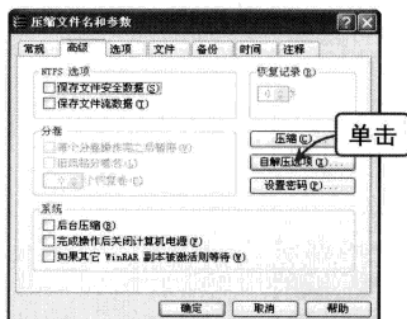
STEP 03 设置高级选项

在“压缩文件名和参数”对话框中选择“高级”选项卡，单击“自解压选项”按钮，如下图所示。

STEP 04 设置解压前后运行的程序

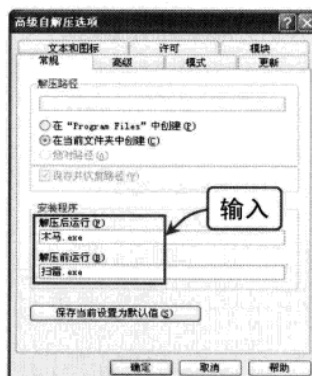
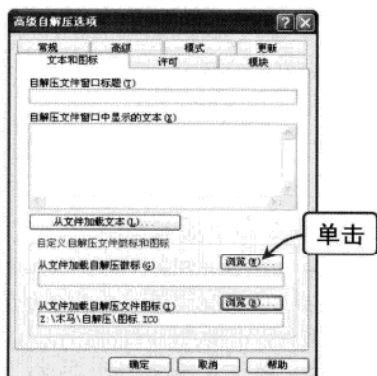
在弹出的“高级自解压选项”对话框中选择“常规”选项卡，选中“在当前文件夹中创建”单选按钮，分别输入解压后运行和解压前运行的文件名，如下图所示。

黑客
基础
知识
常用
扫描
与嗅探
工具
Windows
系统
漏洞
攻防
设置
系统
安全
策略
系统
与文
件加密
远程
控制
木马
聊天
软件
网页
恶意
代码
攻防
电子
邮件
安全
软件
使用
电脑
黑客
技巧



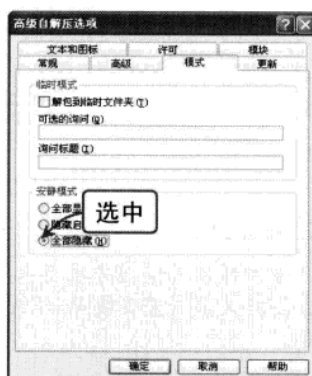
STEP 05 设置自解压文件图标

选择“文本和图标”选项卡，单击“浏览”按钮，从文件加载自解压文件的图标，如下图所示。



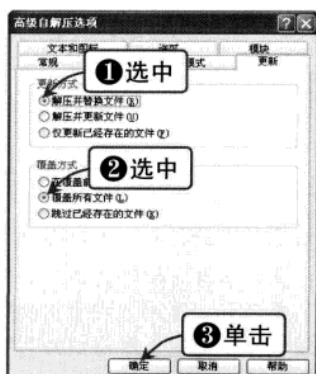
STEP 06 设置自解压文件模式

选择“模式”选项卡，在“安静模式”选项区中选中“全部隐藏”单选按钮，如下图所示。



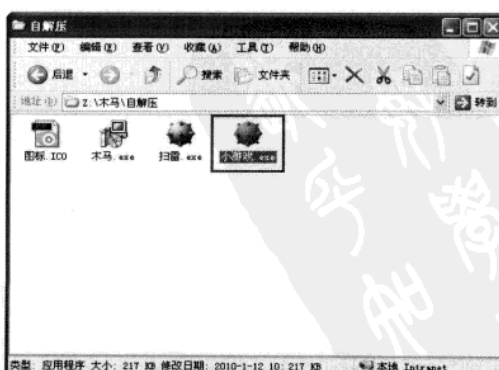
STEP 07 设置自解压文件更新

选择“更新”选项卡，在“更新方式”选项区中选中“解压并替换文件”单选按钮；在“覆盖方式”选项区中选中“覆盖所有文件”单选按钮，单击“确定”按钮，如下图所示。



STEP 08 自解压文件完成

自解压文件创建完毕后，会在指定目录生成一个新的指定名称和图标的可执行文件，如下图所示。当运行小游戏文件时，用户看到的是打开扫雷游戏，但是木马程序已经在后台运行了。



Work2 自解压木马的查杀

如果用户遇到疑似木马的使用 WinRAR 软件生成的执行文件，怎么进行查杀呢？方法有两种：一种是主动式，一种是被动式。

主动式就是如果怀疑某个文件是木马程序，或者不确定某个文件是否为木马程序，先不要双击鼠标执行。一定要先在计算机系统中安装 WinRAR 软件，然后在疑似木马的执行文件上右击，在弹出的快捷菜单中如果有“用 WinRAR 打开”选项，就说明这个文件一定是使用 WinRAR 软件生成的自解压执行文件。选择“用 WinRAR 打开”选项，用 WinRAR 打开执行文件，判断是否有可疑文件，再进行下一步操作。

被动式就是使用常用的一些杀毒软件或木马专杀工具进行查杀。



提示

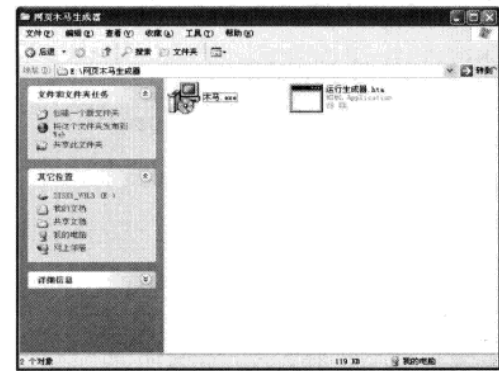
WinRAR 软件是目前使用最多的压缩工具，建议用户在计算机中一定要安装这个软件。这样不但能够解决日常文件的压缩/解压缩问题，更主要的是能够对不确定是否安全的 RAR 压缩文件进行手工检查。

7.2.3 网页木马生成器

网页木马的实质是利用漏洞向用户传播木马下载器，表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文件中，当有人访问时网页木马就会利用对方系统或者浏览器的漏洞自动将配置好的木马的服务端下载到访问者的电脑上来自动执行。下面将介绍具体的制作方法。

STEP 01 准备程序

首先，应下载一个网页木马生成器程序和一个准备好的木马程序，如下图所示。

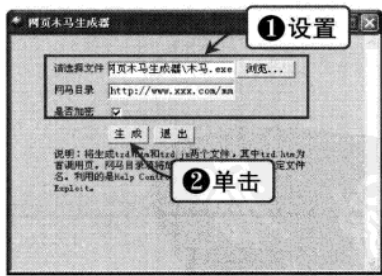


STEP 03 生成文件

在弹出的提示信息框中单击“确定”按钮，则生成相应的网页木马文件，如下图所示。

STEP 02 程序配置

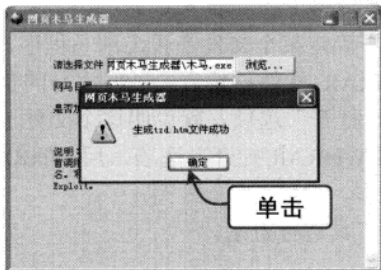
运行网页木马生成器，在“请选择文件”文本框中输入木马程序的位置，在“网马目录”文本框中输入木马的网页路径，选中“是否加密”复选框，单击“生成”按钮，如下图所示。



STEP 04 上传木马

网页木马生成器将生成 tzd.htm 和 tzd.js 两个文件，其中 tzd.htm 为首调用页。将这两个文件上传到与设置的网页木马地址所对应的网络空间中。若有他人访问该地址时，将会自动感染木马病毒，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



7.2.4 CHM 电子书木马

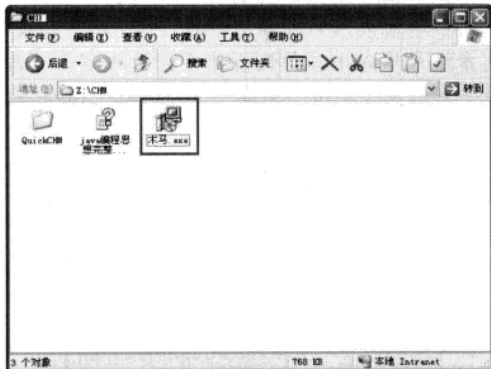
下面将介绍 CHM 电子书木马的制作与查杀方法。

Work1 CHM 电子书木马的制作

网络资源的免费与获得简单等特点使电子书成为网络上传播知识的主要形式之一。同时，在电子书中捆绑木马也更容易欺骗用户，下面将详细介绍如何将木马捆绑在 CHM 格式的电子书中。

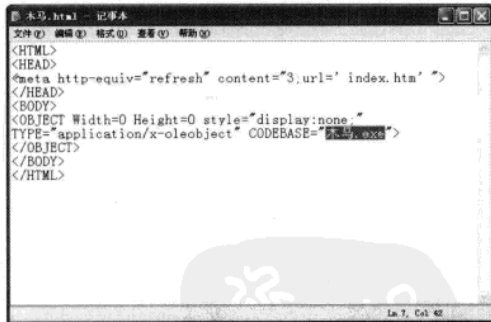
STEP 01 准备文件与木马

在制作 CHM 电子书木马前应首先需要下载和安装一个 QuickCHM 软件，并且准备一个 CHM 电子书文件以及一个木马，如下图所示。



STEP 02 编写网页代码

打开一个记事本文件，编写一个网页代码，需要改动的地方已在图中注明。将其保存为 .html 类型的文件，本例保存为 木马.html，如下图所示。



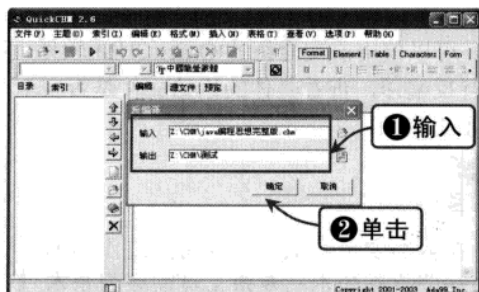
STEP 03 电子书反编译

运行 QuickCHM 软件，单击“文件”|“反编译”命令，在弹出的对话框中选择“输入”和“输出”文件夹，在“输入”项中选择电子书路径，在“输出”项中选择反编译后的文件存储路径（本例输出路径为 Z:\CHM\测试），单击“确定”按钮，如下图所示。

STEP 04 找到扩展名为 .hhp 文件

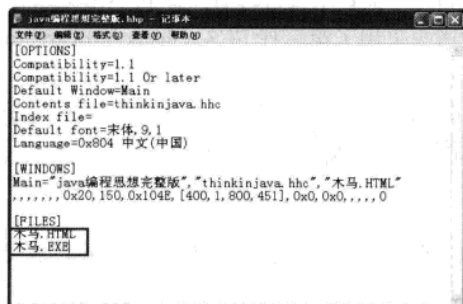
反编译完成后会弹出反编译文件夹，找到其中扩展名为 .hhp 的文件，也就是和电子书名称相同的那个文件。本例中是名为“java 编程思想完整版.hhp”的文件，如下图所示。

Chapter 07 木马攻防



STEP 05 修改.hhp 文件

用记事本打开“java 编程思想完整版.hhp”文件，在[WINDOWS]小节的“Main=”后添加“木马.html”。在[FILES]小节添加“木马.HTML”和“木马.EXE”并保存，如下图所示。



STEP 07 重新编译 CHM 文件

再次运行 QuickCHM 软件，单击“文件”|“打开”命令，弹出“打开”对话框，选择刚刚修改过的“java 编程思想完整版.hhp”文件，单击“打开”按钮，如下图所示。



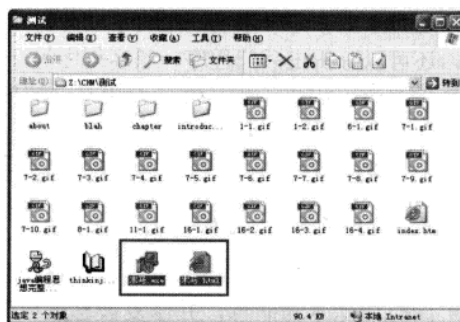
Work2 CHM 电子书木马的查杀

CHM 电子书木马是依托 CHM 文件格式存在的，有很大的局限性，只要平时对 CHM 文



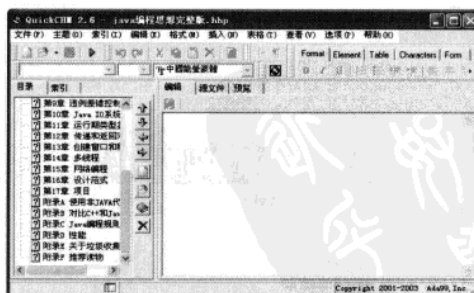
STEP 06 添加木马文件

将前面编写的网页文件（木马.html）和木马文件（木马.exe）复制到反编译后的文件夹中，如下图所示。



STEP 08 重新编译完成

单击“文件”|“编译”命令，稍等片刻编译完成，弹出对话框显示“完成！你希望运行吗？”，单击“否”按钮，此时已完成了一个 CHM 电子书木马的制作，如下图所示。



基础知
识

与嗅探工
具

统漏洞攻
防

安全策
略

系统与文
件加密

远程控
制

木马
攻防

聊天软
件攻防

网页恶
意代码攻
防

电子邮
件攻防

C盘病
毒攻防

使用电
脑安全软
件

黑客攻
防技巧



件多加注意就可以了。下载电子书可以在一些比较正规的大站点进行，因为这里的书籍一般都是他们自己制作的，相对安全性要高一些。

如果不确定要打开的 CHM 电子书是否安全，可以使用前文介绍的 QuickCHM 软件（类似 CHM 文件编辑软件都可以）对 CHM 文件进行反编译，查看具体的原始文件是否安全，或者直接使用常见的杀毒软件对 CHM 文件进行手工查杀。

7.3 木马的清除与防范

面对形形色色的木马，用户应该提高自身的安全意识，做好防范工作。即使中了木马也不要过于惊慌，还可以通过一些优秀的木马专杀工具彻底查杀木马的。

7.3.1 木马清道夫清除木马

Windows 木马清道夫是一款专门查杀并可辅助查杀木马的专业级反木马信息安全产品。它可自动查杀上百万种木马，配合手动分析几乎可 100% 对未知木马进行查杀。它不仅可查木马，还可以分析出后门程序、黑客程序等。木马清道夫采用了第三代 FCS（fastcontrolstream，高速控制流）扫描引擎，准确率更高，速度提升一倍，占用资源更少，具有多目的扫描、可疑模块探测、木马防御、木马监控等先进功能。其专业的分析木马能力、完美的升级能力成为用户清除木马病毒的首选。木马清道夫官方网站地址为 <http://www.mmsk.cn>。

Work1 进行多方位扫描

木马清道夫可通过扫描进程、扫描硬盘、扫描注册表等多方位扫描进行木马病毒的探查，并可同时清除木马病毒，并修复被恶意更改的注册表项目。

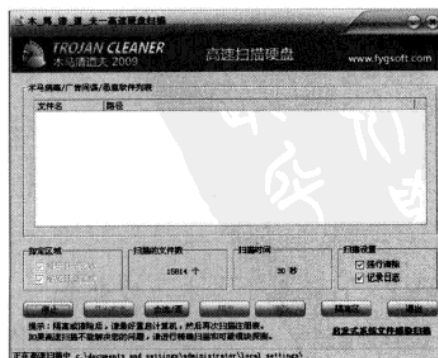
STEP 01 扫描进程

在木马清道夫主窗口中单击“扫描进程”按钮。在“扫描进程”窗口中单击“扫描”按钮，可以扫描系统进程中的可疑木马病毒，如果发现病毒，可单击“清除”按钮清除，如下图所示。



STEP 02 高速硬盘扫描

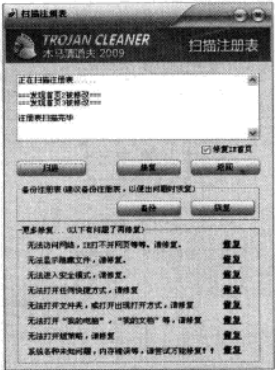
在木马清道夫主窗口中，单击“扫描硬盘”按钮。在“高速硬盘扫描”窗口中单击“扫描”按钮，能够较快扫描特定区域和敏感区域，迅速定位木马病毒文件，如果发现病毒，可单击“隔离”或“清除”按钮，对病毒进行隔离或清除，如下图所示。



Chapter 07 木马攻防

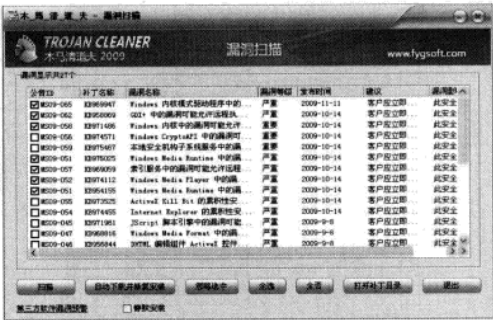
STEP 03 扫描注册表

在木马清道夫主窗口中单击“扫描注册表”按钮，在“扫描注册表”窗口中单击“扫描”按钮，开始扫描系统注册表的错误和被恶意修改的项目，如果已被木马修改，单击“修复”按钮即可自动修复，如下图所示。



STEP 04 漏洞扫描

在木马清道夫主窗口中单击“漏洞扫描”按钮，在“漏洞扫描”窗口中单击“扫描”按钮。扫描完毕后，在列表中显示需要修复的漏洞，选中需要修复漏洞的复选框，单击“自动下载并修复安装”按钮即可修复，如下图所示。

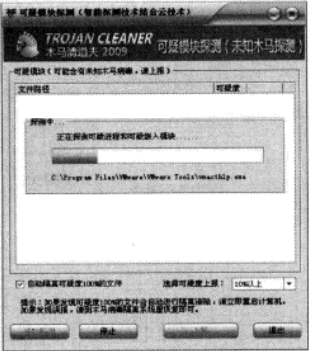


Work2 可疑模块探测

可疑模块探测的主要功能是智能分析内存中驻留的程序并进行处理，分析出可疑程序或可疑模块，并可对系统做出全面诊断分析报告。

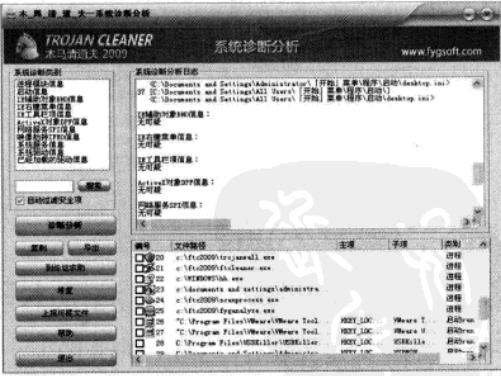
STEP 01 探测可疑模块

在木马清道夫主窗口中单击“可疑模块探测”按钮，在“可疑模块探测”窗口中单击“开始探测”按钮，可以探测出系统进程中的可疑程序并列出其可疑度，供用户分析参考，如下图所示。



STEP 02 系统诊断分析

在木马清道夫主窗口中单击“可疑模块探测”按钮，在“系统诊断分析”窗口中单击“诊断分析”按钮，在右窗格中会显示具体的系统分析报告，如下图所示。



Work3 木马清道夫防火墙

木马清道夫防火墙通过进行多层木马监控和防御，可有效阻止木马的进入。木马清道夫防火墙的使用方法如下：

基础知识

常用扫描工具

系统漏洞攻防

设置系统安全策略

系统与文件加密

远程攻击

木马攻防

聊天软件

网页恶意代码

电子邮件

C盘病毒

使用电脑安全软件

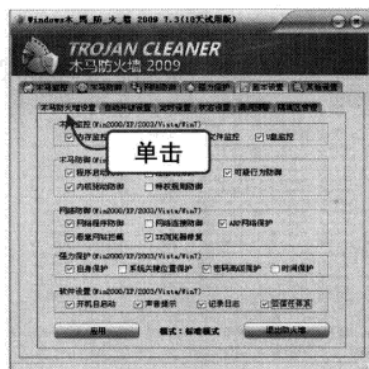
黑客攻防

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



STEP 01 基本设置

在木马清道夫主窗口中单击“木马防火墙”按钮，在“木马防火墙”窗口中可以根据用户需要，通过选中项目名称前的复选框的形式，分别开启“木马监控”、“木马防御”、“网络防御”、“强力保护”和“软件设置”各项功能，如下图所示。



STEP 02 实时监控

在“木马防火墙”窗口中，单击“木马监控”选项卡中的“实时监控”项，可以查看实时监控的进程，并可对可疑文件进行隔离或清除，如下图所示。



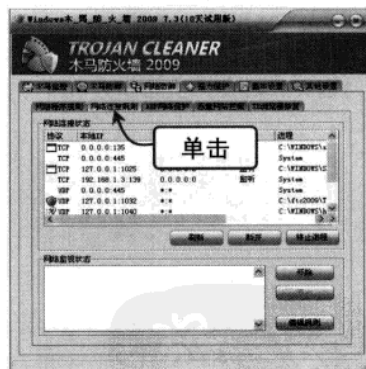
STEP 03 程序防御规则

在“木马防火墙”窗口中，单击“木马防御”选项卡中的“程序防御规则”选项，通过添加“允许列表”，可拦截未知木马病毒通过捆绑方式、自动下载方式、自动运行方式入侵或感染系统，如下图所示。



STEP 04 网络连接规则

在“木马防火墙”窗口中，单击“网络防御”选项卡中的“网络连接规则”选项，即可以监视应用程序访问网络所使用的数据传输通信协议、端口等。如发现不正常的进程，可单击“终止进程”按钮或“断开”按钮，如下图所示。



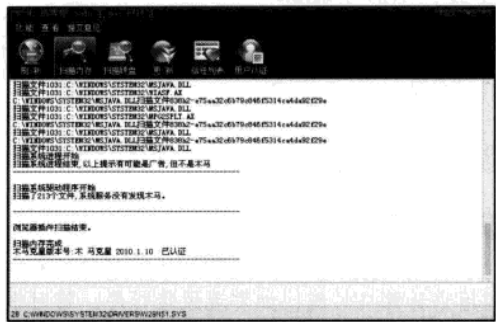
7.3.2 木马克星 Iparmor 清除木马

木马克星是一款适合于网络用户的安全软件，既有面向新手的扫描内存和扫描硬盘功能，也有面向网络高手的众多调试查看系统功能。Iparmor 系列内置木马防火墙，任何黑客试图与本机可疑端口建立连接，都需要 Iparmor 确认，包括邮件监视技术、QQ 密码偷窃以及 getpass 密码邮寄均需要 IParmor 确认，最大程度保证了用户的网络安全。木马克星官方网站地址为 <http://www.luosoft.com>。

Chapter 07 木马攻防

STEP 01 扫描内存

木马克星软件运行后，自动进行内存扫描，直观显示了当前内存中是否存在木马、是否有可疑程序监视键盘输入，并且可以自动杀查内存中的木马，不需要人工干预，同时显示扫描文件数量和扫描结果，如下图所示。



STEP 02 扫描硬盘

在“木马克星”窗口中单击“扫描硬盘”按钮，可以扫描硬盘中是否存在木马病毒，并可对可疑文件进行隔离或删除，如下图所示。



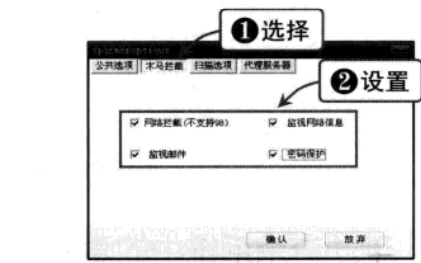
STEP 03 升级病毒库

木马病毒种类和数量更新频繁，建议用户每隔 2~3 天应升级一次病毒库。在“木马克星”窗口中单击“更新”按钮进入软件升级界面，单击“开始”按钮开始升级，如下图所示。



STEP 04 设置木马拦截选项

在“木马克星”窗口中，选择“功能”|“设置”选项，选择“木马拦截”选项卡。可根据用户需要选择不同的拦截种类，如下图所示。



7.3.3 金山贝壳木马专杀清除木马

根据云安全统计数据显示，每日有上百万用户机器被新木马/病毒感染，其中网络游戏盗号类木马占 80%。贝壳木马专杀是国内首款专为网游防盗号量身打造的，是一款完全免费的木马专杀软件；其安全检测采用云计算技术，拥有世界最大的云安全数据库，能在 5 分钟内快速识别新木马/病毒，保证系统、账号、用户隐私安全。贝壳木马专杀官方网站地址为 <http://www.beike.cn>。

STEP 01 开始查杀

贝壳木马专杀运行后，提供了三种扫描方式：快速扫描、全盘扫描和自定义目录扫描。选中“快速扫描”单选按钮，单击“开始查杀”按钮，如下图所示。

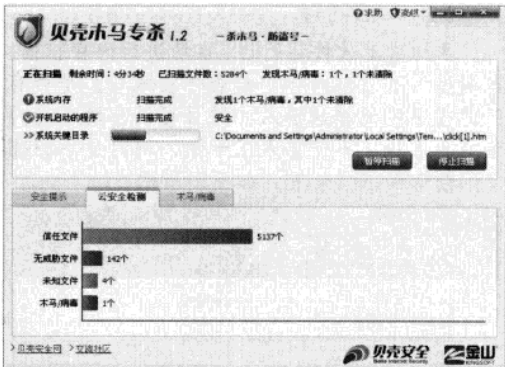
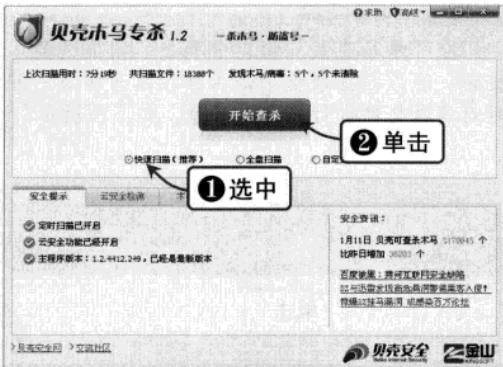
STEP 02 查杀过程

在贝壳木马专杀扫描文件过程中，实时显示扫描的文件数量以及木马数量，并同时提供云安全检测结果，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



黑客攻防从新手到高手

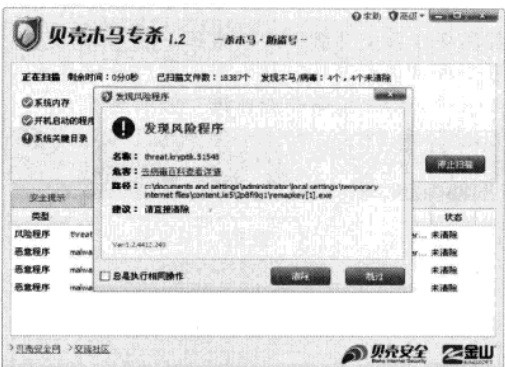
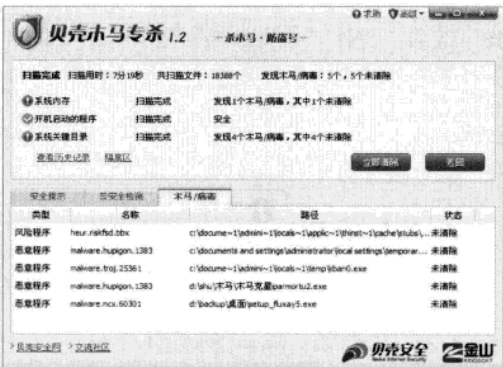


STEP 03 查杀结果

查杀完后，分别显示“系统内存”、“开机启动程序”、“系统关键目录”的扫描情况，并列出的病毒名称和所在路径，如下图所示。

STEP 04 实时监控

贝壳木马专杀的实时监控功能能够随时监控用户计算机系统，如发现风险程序，随时报告并提供解决意见，如下图所示。



7.3.4 手动查杀系统中的隐藏木马

用户被植入木马程序后，如果没有木马专杀工具，或木马专杀工具没有彻底清除木马病毒时，我们就可以采用手动查杀的方式，找到木马程序常在的几个藏匿之处，进行手动清除。

- ❖ 单击“开始”|“运行”命令，输入 msconfig 命令查看启动项和服务项，非必要性的启动和服务都禁用。
- ❖ 检查注册表。单击“开始”|“运行”命令，输入 regedit 命令打开注册表，查看注册表中是否有可疑的启动项，如：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
```


Chapter 07 木马攻防

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders

一般注册表启动为以上几项，如发现可疑启动项就可删除，也可以打开键值找到相应的文件路径，将其文件删除。当然，不要忘了删除注册表相应选项，否则开机提示找不到相应文件。

❖ 查看并删除临时文件，如：

C:\temp\

C:\Windows\prefetch

C:\Documents and Settings\用户名\local setting\Temporary Internet Files

C:\Documents and Settings\用户名\Templates

C:\Program Files\Internet Explorer\PLUGINS

❖ 查看系统进程文件如 win.ini, system.ini。

在 win.ini 文件的[WINDOWS]字段中有启动命令“load=”和“run=”，在一般情况下“=”后面是空白的，如果有后跟程序，例如，run=c:\Windows\GAME.exe load=c:\Windows\GAME.exe 那么 GAME.exe 这个文件就是木马了。应修改还原为默认值，将 run=“木马程序”或 load=“木马程序”更改为“run=”和“load=”。

在 system.ini 文件中，在[boot]字段下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell=explorer.exe 程序名”，那么后面跟着的那个程序就是“木马”程序，就是说你已经中“木马”了。应修改还原为默认值，将[boot]字段下面的“shell=木马文件”，更改为：“shell=explorer.exe”。

7.3.5 常见木马防范措施

木马要发挥作用，必须先将木马服务器程序植入到目标计算机中，然后打开一个监听端口与控制端建立连接。因此，预防木马最好的办法是修正系统配置，科学管理计算机各个端口，关闭无用端口，不运行来历不明的程序，及时修复系统漏洞，从根本上杜绝木马程序的侵入。下面将介绍几种常见的木马预防方法。

Work1 关闭易攻击端口

1. 关闭 135 端口

135 端口在 Windows 默认的五個典型开放端口中，用途最为复杂，也最容易引起外部攻击。该端口对应的 RPC 服务是 Windows 操作系统使用的一个远程过程调用协议。RPC 提供了一种进程间的通信机制，通过这一机制，允许在某台计算机上运行的程序顺畅地在远程系统上执行代码。攻击者能利用该漏洞在受影响的系统上以本地系统权限运行代码，执行任何操作，包括安装程序，查看、更改或者删除数据，或者建立系统管理员权限的账户。避免这种危险的最好办法是关闭 RPC 服务。

2. 关闭 137 和 138 端口

137 端口是 Windows 网络通信协议 NetBIOS over TCP/IP (NBT) 的计算机名管理功能中使用的端口。连入局域网的主机，只需向对方 Windows 的 137 端口发送一个询问连接状态的信息包，就可以得到该机的计算机名和注册用户名，该机是否为主域控制器和主浏览器、

基础知识

与嗅探工具

系统漏洞攻防

安全策略

系统加密

远程控制

木马

聊天软件

网页恶意

电子邮件

C 盘病毒

使用电脑

黑客技巧



是否作为文件服务器使用、IIS 和 Samba 是否正在运行以及 Lotus Notes 是否正在运行等信息。不只是局域网内部，连接因特网的电脑也是如此。只要知道对方的 IP 地址，就可以向这台电脑的 137 端口发送一个请求，获得诸多信息，从而进行攻击活动。

138 端口提供 NetBIOS 的浏览功能。在该功能中，被称为主浏览器的电脑管理着连接于网络中的电脑一览表的浏览列表。该功能使用的是与 137 端口计算机名管理不同的运行机制，主要用来显示连接于网络中的电脑一览表。每台电脑在启动时或连接网络时都会利用 138 端口广播自己的 NetBIOS 名，将自己的电脑信息发送给同组中的所有电脑。收到 NetBIOS 名的主浏览器会将这台电脑追加到浏览列表中。需要显示一览表时就广播一览表显示请求，收到请求的主浏览器会发送浏览列表。关闭电脑时，机器会通知主浏览器，以便让主浏览器将自己的 NetBIOS 名从列表中删除掉。尽管 138 端口的信息量没有 137 端口那么多，但也存在不容忽视的安全隐患。

3. 关闭 139 和 445 端口

139 和 445 端口的功能主要是通过 137 和 138 端口获取 IP 地址，实现文件共享和打印机共享等。139 和 445 端口的通信过程是通过 SMB（服务器信息块）协议实现的，即根据 DNS 服务器中的名字列表信息，寻找需要通信的对象。如果顺利地得到对象的 IP 地址，就可以访问共享资源。Windows 2000 以前版本的 Windows 使用 NetBIOS 协议解决各计算机名的问题。通过向 WINS 服务器发送通信对象的 NetBIOS 名，取得 IP 地址。如果取得了用户的 IP 地址，攻击者就可以进行攻击行为，因此这两个端口也需要关闭。

4. 关闭 1900 端口

1900 端口对应的是 SSDP Discovery Service 服务。攻击者只要向某个拥有多台 Windows XP 系统的网络发送一个虚假的 UDP 包，就可能会造成这些 Windows XP 主机对指定的主机进行攻击（DDOS）。另外如果向该系统 1900 端口发送一个 UDP 包，令 Location 域的地址指向另一系统的 chargen 端口，就有可能使系统陷入一个死循环，消耗掉系统的所有资源。

以上只是列举了几个比较容易受攻击的端口，单单靠关闭端口的办法是不能彻底杜绝木马程序的进攻的，还需要用户在平时养成良好的计算机使用习惯，提高自我安全防范意识，才能真正做到防患于未然，将木马攻击伤害降到最低。

Work2 良好的计算机日常使用习惯

- ❖ 定期升级 IE，并将 IE 的 Internet 选项中的“高级”设置为“恢复默认设置”，这将过滤一些非法、不安全的网站。

- ❖ 不下载和执行任何来历不明的软件。对于从网上下载的软件在安装、使用前一定要用几种反病毒软件，最好是专门查杀木马的软件进行检查，确定无毒后再执行、使用。

- ❖ 及时修补系统漏洞。应做到及时安装和更新相应的系统补丁程序，防止木马通过漏洞在系统上打开端口留下后门，上传木马文件和执行代码。

- ❖ 尽量少使用共享文件夹。如果必须使用共享文件夹，则最好设置账号和密码保护。注意千万不要将系统目录设置成共享，最好将系统默认共享的目录关闭。Windows 系统默认情况下将目录设置成共享状态，这是非常危险的。

- ❖ 不打开来历不明的邮件。现在许多木马都是通过邮件来传播的，当你收到来历不明的邮件时，请不要打开，应尽快删除，并加强邮件监控系统，拒收垃圾邮件。

- ❖ 将 Windows 资源管理器配置成始终显示扩展名。因为一些扩展名为 VBS、SHS、PIF 的文件多为木马病毒的特征文件，更有些文件没有扩展名，那更应重点查看，一经发现要立即删除，千万不要打开，只有实时显示了文件的全名才能及时发现。
- ❖ 使用代理服务器，隐藏自己的真实 IP 地址。
- ❖ 运行实时监控。在上网时最好运行反木马实时监控程序和个人防火墙，并定时对系统进行病毒检查。
- ❖ 经常升级系统和更新病毒库。开启实时更新升级功能，定时修复系统漏洞和更新杀毒软件的病毒库。

7.4 “冰河”木马的使用

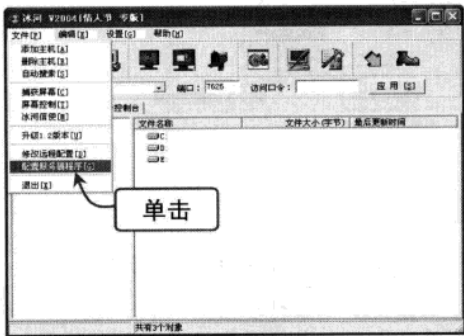
冰河是一个国产木马，在国内流行极广，几乎每一百台电脑就有两三台寄存着该木马，有些地方比例会更高，尤其是网吧。种下这个木马的攻击者能完全控制用户的电脑，它具有自动跟踪目标机屏幕变化、记录各种口令信息、获取系统信息、限制系统共享、远程文件操作、注册表操作等功能，危险性极高。下面就来认识冰河木马以及清除方法。

7.4.1 配置“冰河”木马的服务器端程序

冰河木马的主程序包括两部分：服务端和控制端。服务端需要在被控制的电脑上执行。当控制端连接服务端主机后，控制端会向服务端主机发出命令。而服务端主机在接受命令后，就会执行相应的任务。下面将介绍如何配置服务端程序。

STEP 01 进入配置服务器程序

运行冰河木马主程序后，单击“文件”|“配置服务器程序”命令，如下图所示。



STEP 02 基础设置

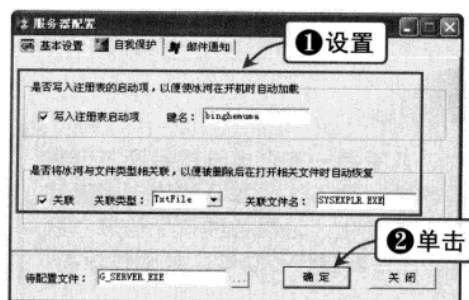
在服务器配置窗口选择“基本设置”选项卡，选择木马安装的系统目录，输入木马安装后的文件名称，输入隐藏的进程名称，输入访问口令，输入木马运行后的提示信息，输入监听端口号，选中“自动删除安装文件”复选框，单击“确定”按钮，如下图所示。





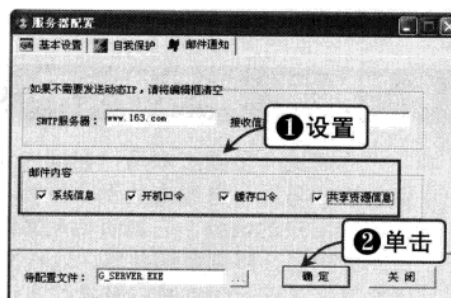
STEP 03 自我保护

在服务器配置窗口选择“自我保护”选项卡，选中“写入注册表启动项”复选框，并填写相应的键名，就可以随被攻击的计算机系统一起启动。选中“关联”复选框，选择关联类型，输入关联文件名。一旦冰河木马被删除后，可通过启动已关联类型的文件再次启动。单击“确定”按钮，如下图所示。



STEP 04 邮件通知

在服务器配置窗口，选择“邮件通知”选项卡。如想接收已经被种植木马的计算机基本信息，可填写接收邮箱地址，并在“邮件内容”选项区选择接收被控制计算机的何种信息。单击“确定”按钮，如下图所示。

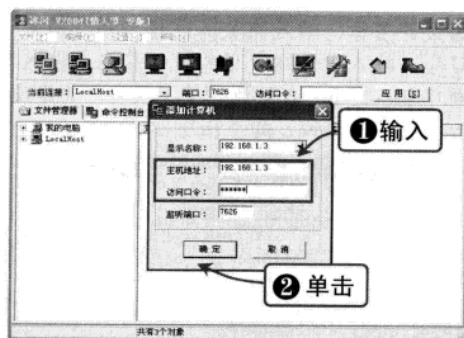


7.4.2 使用“冰河”木马控制远程计算机

使用冰河木马程序可以对已经植入服务端的计算机进行文件管理、控制屏幕、设置共享、获取系统信息等多种操作，下面将介绍几种常见的远程操作功能。

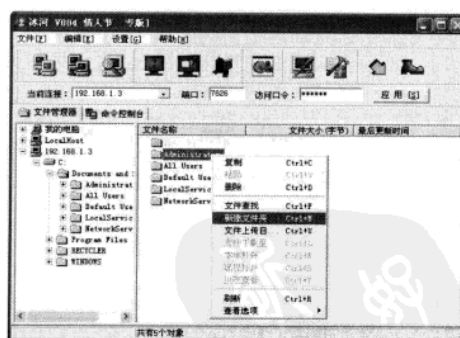
STEP 01 输入主机地址以及访问口令

运行冰河木马主程序后，单击“文件”|“添加主机”命令，在弹出的对话框中输入主机地址以及访问口令，单击“确定”按钮，连接到服务端计算机，如下图所示。



STEP 02 选择“文件管理器”选项卡

在冰河木马控制端主窗口中选择“文件管理器”选项卡，显示了服务端计算机的所有文件，对这些文件控制端可以实现进行远程复制、删除、共享上传等操作，如下图所示。



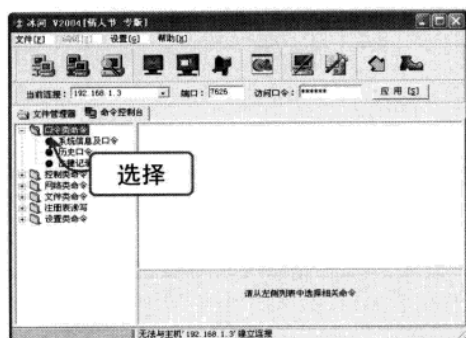
STEP 03 选择“口令类命令”选项

在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“口令类命令”选项，根据各种命令可以对服务端计算机进行获取系统信息和历史口令以及记录键盘等操作，如下图所示。

STEP 04 选择“控制类命令”选项

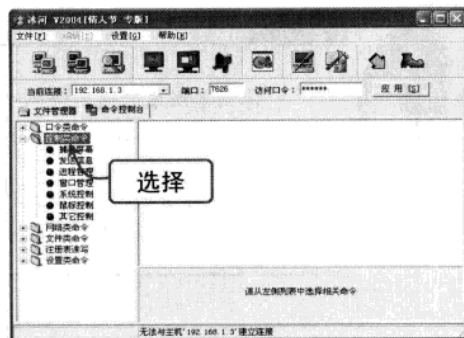
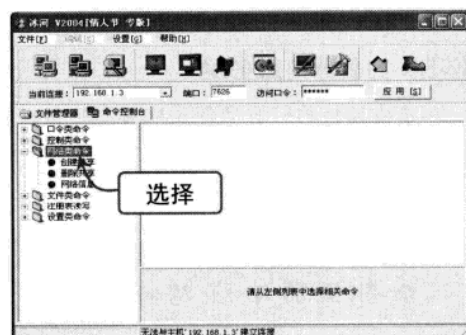
在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“控制类命令”选项，根据各种口令，可以对服务端计算机进行捕捉屏幕、发送信息、进程管理、鼠标控制等操作，如下图所示。

Chapter 07 木马攻防



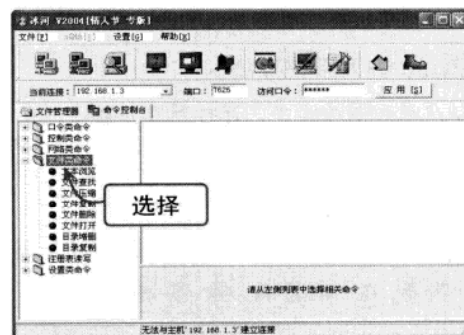
STEP 05 选择“网络类命令”选项

在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“网络类命令”选项，根据各种命令，可以对服务端计算机进行创建共享、删除共享、查看网络信息等操作，如下图所示。



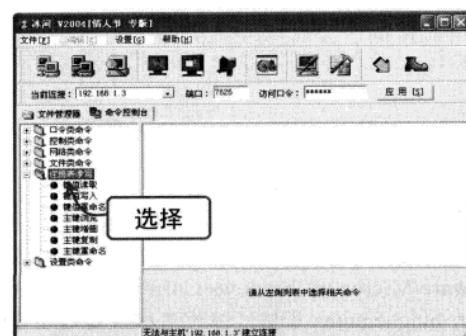
STEP 06 选择“文件类命令”选项

在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“文件类命令”选项，根据各种命令，可以对服务端计算机中的文件进行查找、压缩、复制、上传等操作，如下图所示。



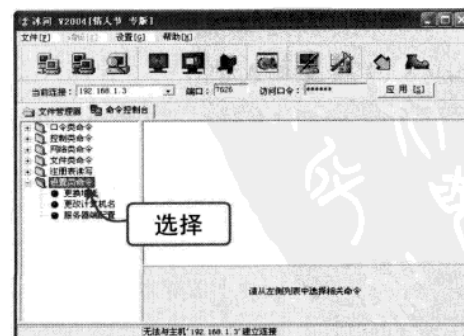
STEP 07 选择“注册表读写”选项

在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“注册表读写”选项，根据各种命令，可以对服务端计算机的注册表进行读写、重命名等操作，如下图所示。



STEP 08 选择“设置类命令”选项

在冰河木马控制端主窗口中，选择“命令控制台”选项卡中的“设置类命令”选项，根据各种命令可以对服务端计算机设置进行修改和重新配置，如下图所示。



基础知识

与嗅探工具

系统漏洞攻防

设置系统

系统安全

远程控制

木马攻防

代码攻防

电子取证

病毒攻防

安全软件

实用技巧



提示

冰河各版本的通用密码：
2.2 版：Can you speak Chinese? 或 05181977
3.0 版：yzkzero! 3.1-netbug 版密码：123456!
2.2 杀手专版：dzq20000! 2003 牛族专版：05031980
2004 情人节专版：05031980

7.4.3 卸载和清除“冰河”木马

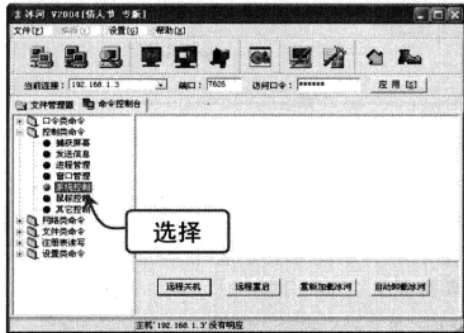
前面着重介绍了冰河木马的使用，如果用户不小心被植入了冰河木马，也不用过于担心，可以通过以下方法进行卸载和清除。

Work1 使用控制端程序卸载

使用控制端程序可以对冰河木马进行本地或远程卸载，下面以远程卸载为例，具体操作方法如下：

STEP 01 进入系统控制

启动控制端程序，连接到服务器端。在控制端主程序窗口中选择“命令控制台”选项卡，选择“控制类命令”|“系统控制”选项，如下图所示。



STEP 02 卸载冰河服务端

单击右窗格的“自动卸载冰河”按钮，在弹出的提示信息框中单击“是”按钮，冰河木马的服务器端即被清除，如下图所示。



Work2 清理注册表

用户可以通过清理注册表和恢复关联文件属性的方法删除冰河木马程序，具体操作方法如下：

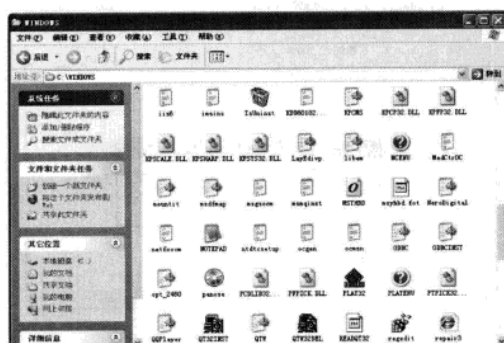
STEP 01 删除木马文件

删除 C:\WINDOWS 目录下的 Kernel32.exe 和 Sysexplr.exe 文件，如下图所示。

STEP 02 清理 Run 子键

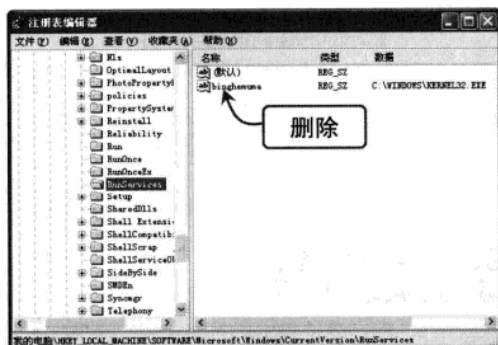
删除注册表 HKEY_LOCAL_MACHINE\software\Microsoft\Windows\CurrentVersion\Run 中的 binghemuma 子键（键值名称为 C:\WINDOWS\KERNEL32.EXE），如下图所示。

Chapter 07 木马攻防



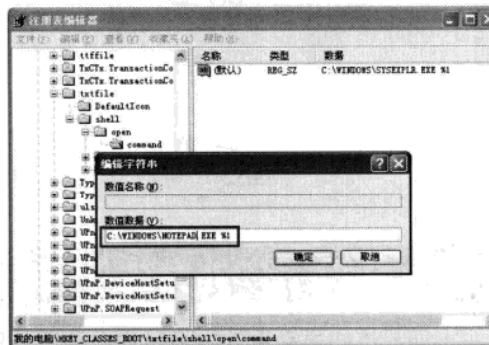
STEP 03 清理 RunServices 子键

删除注册表 HKEY_LOCAL_MACHINE\software\Microsoft\Windows\CurrentVersion\RunServices 中的 binghamuma 子键（键值名称为 C:\WINDOWS\KERNEL32.EXE），如下图所示。



STEP 04 恢复文件关联

修改注册表 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的默认值，由中木马后的 C:\WINDOWS\SYSTEM\SYSEXPLR.EXE %1 改为正常情况下的 C:\WINDOWS\notepad.exe %1，即可恢复 TXT 文件关联功能，如下图所示。



提示

目前，一些常见病毒和木马经常会篡改常用文件的关联方式，用户要学会手工进行恢复。相信在工作和学习生活中一定会用到的。

Work3 使用“冰河陷阱”

“冰河陷阱”是冰河木马开发者提供的专用来查杀和卸载冰河木马程序的工具，下面将介绍如何使用“冰河陷阱”。

STEP 01 运行冰河陷阱

下载“冰河陷阱”后，直接运行主程序，如下图所示。

STEP 02 确认删除

运行“冰河陷阱”程序后，会自动检测用户是否被植入冰河木马，如果检测到将弹出提示信息框，单击“是”按钮，如下图所示。

基础知识

与嗅探工具

系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制攻防

木马攻防

聊天软件攻防

网页恶意代码攻防

电子邮件攻防

使用电脑安全软件

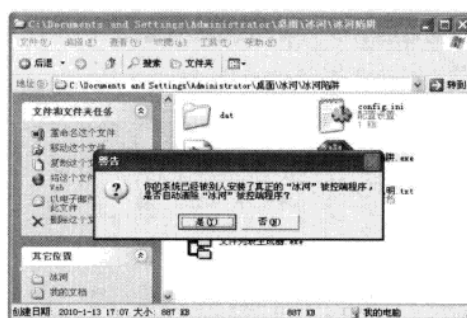
黑客攻防实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



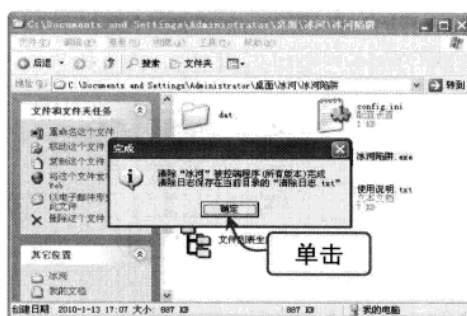
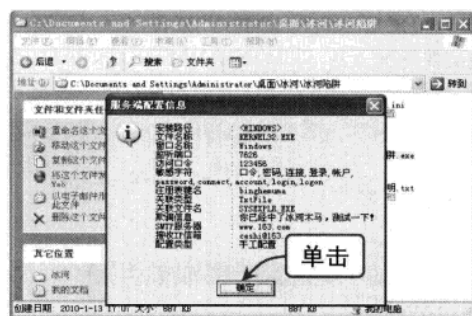
STEP 03 确认配置信息

弹出服务器配置提示信息框，提示冰河木马的基本配置信息，单击“确定”按钮，如下图所示。



STEP 04 清除完成

木马被控制端程序被清除后，弹出提示信息框，单击“确定”按钮，如下图所示。



7.5 认识“广外女生”木马与清除该木马

“广外女生”木马是广东外语外贸大学“广外女生”网络小组开发的一种木马程序。它能够实现远程监控的各种功能，包括远程修改注册表、进行文件删改和上传以及屏幕控制，具有服务端程序体积小、占用系统资源少、隐蔽性好的特点。并且能利用 Windows 的漏洞使国内流行的“天网防火墙”和“金山毒霸”失去作用。

7.5.1 “广外女生”木马的使用

从网络上下载“广外女生”木马程序，在此使用的是 1.53B 版本，程序只有一个 gwg.exe 文件，这是“广外女生”木马程序控制端。首先要用控制端生成服务端，具体使用方法如下：

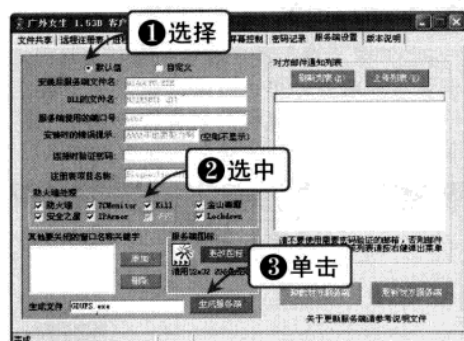
STEP 01 服务端配置

运行“广外女生”，在“广外女生”客户端程序窗口中选择“服务端设置”选项卡，选中“默认值”单选按钮，在“防火墙处理”选项区中选中需要关闭的防火墙（建议全选），单击“生成服务端”按钮，如下图所示。

STEP 02 生成服务端

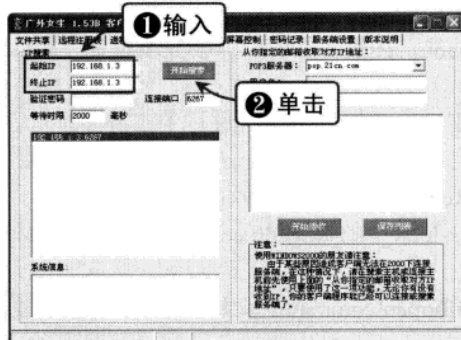
在指定的位置生成了服务端程序（本例中的服务端程序为 GDUFS.exe），用户可以把此服务端程序植入到要攻击的电脑中去，如下图所示。

Chapter 07 木马攻防



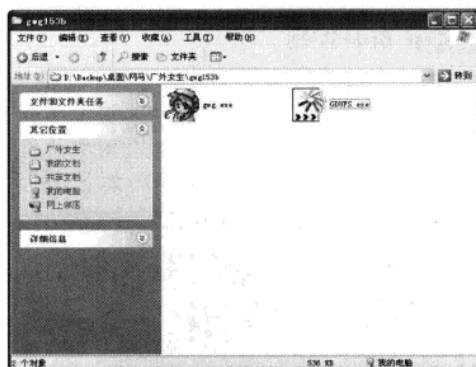
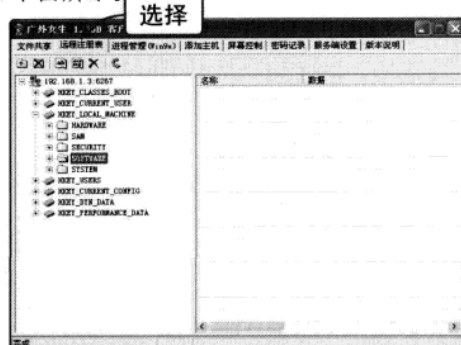
STEP 03 添加主机

服务端程序发布后，就可以通过搜索 IP 范围的方法来查找已经被植入服务端程序的计算机。分别输入起始和终止的 IP 范围，单击“开始搜索”按钮，就会自动搜索已经运行服务端的计算机，如下图所示。



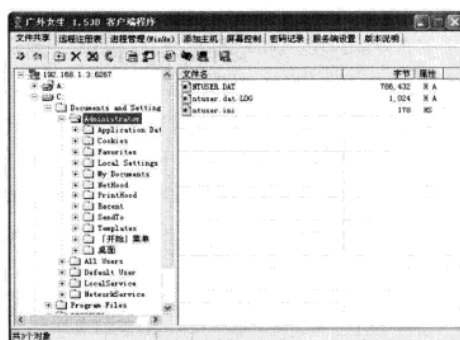
STEP 05 远程注册表

在“广外女生”客户端程序窗口中选择“远程注册表”选项卡，可以对服务端计算机的注册表进行远程操作，以达到控制计算机的目的，如下图所示。



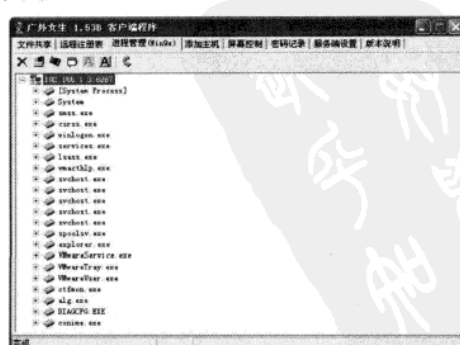
STEP 04 文件共享

在“广外女生”客户端程序窗口中选择“文件共享”选项卡，就可以对服务端计算机中的文件进行修改、删除、上传、设置属性等操作，如下图所示。



STEP 06 进程管理

在“广外女生”客户端程序窗口中选择“进程管理”选项卡，可直接查看服务端计算机的进程列表，并进行停止、添加等操作，如下图所示。



基础知识

与嗅探工具

系统漏洞攻防

设置系统

安全策略

系统与安全

远程攻击

木马

聊天软件

网页恶意

代码攻防

件攻防

电子邮件

C 语言

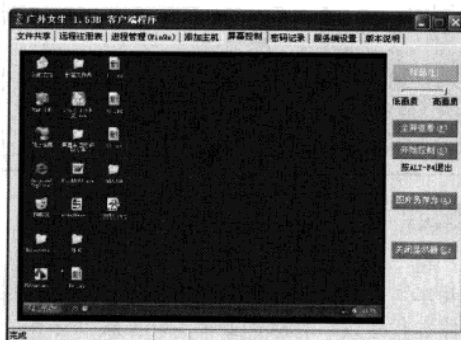
使用电脑

黑客攻防



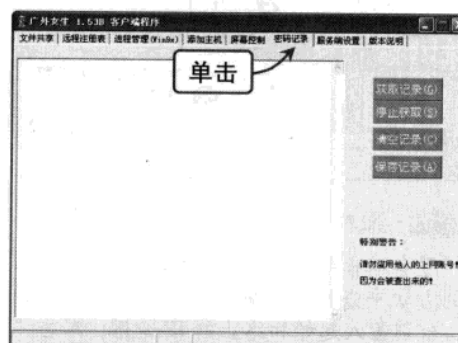
STEP 07 屏幕控制

在“广外女生”客户端程序窗口中选择“屏幕控制”选项卡，就可以直接查看服务端计算机的屏幕动作，甚至可以全屏操作对方的鼠标（包括单击、双击、右击、拖动等），如下图所示。



STEP 08 密码记录

在“广外女生”客户端程序窗口中选择“密码记录”选项卡，单击“获取记录”按钮，就开始记录服务端计算机的所有密码操作，以达到非法获取各种密码的目的，如下图所示。



7.5.2 “广外女生”木马的清除

“广外女生”木马程序本身提供了远程卸载功能，在程序主窗口“服务端设置”选项卡选择“卸载对方服务端”按钮即可。

如果是用户自己感染了“广外女生”木马，则可以使用以下方法进行手工清除：

- ① 启动到纯 DOS 模式下，删除系统 System 目录下的 Diagcfg.exe 文件。
- ② 将系统 Windows 目录中的注册表编辑器 Regedit.exe 改名为 Regedit.com。
- ③ 回到 Windows 模式下，运行系统 Windows 目录中的 Regedit.com 程序（就是刚才改名的文件）。
- ④ 打开 HKEY_CLASSES_ROOT\exefile\shell\open\command 主键，将默认键值改成“%1” %*。
- ⑤ 打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current-Version\RunServices，删除名称为 Diagnostic Configuration 的键值。
- ⑥ 退出注册表编辑器，将 Regedit.com 改回 Regedit.exe。

Chapter

08

聊天软件攻防

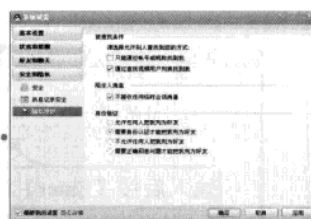
随着计算机网络技术的迅速发展，使用 QQ、MSN 等即时通信软件成为广大网民网络沟通的主要方式。目前，黑客针对即时通信软件的网络攻击也越来越多。下面将介绍几种常见的聊天软件攻击方式和防护措施，以此增强网络安全防范措施。

本章建议学习时间：

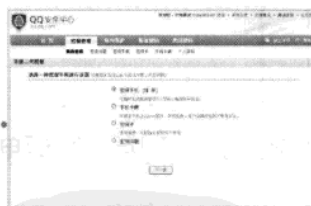
本章建议学习时间为 45 分钟，其中分配 10 分钟学习常见 QQ 攻击方式，25 分钟学习如何保护自己的 QQ，10 分钟学习 MSN 的攻击与防御知识。

学完本章后您可以：

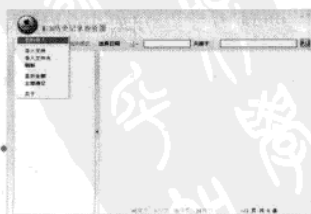
- 了解 QQ 常见攻击方式
- 设置 QQ 密码保护
- 防范 QQ “炸弹”
- 常见 QQ 信息防护措施
- MSN 的攻击和防御



不接收任何临时会话消息



选择密保手段



选择 MSN 历史记录存放位置



重要知识点视频索引



8.1 常见 QQ 攻击方式

QQ 作为主流的即时通讯工具之一，随着功能的进一步增强，某些薄弱环节也逐渐暴露，成为黑客攻击的漏洞。下面将介绍几种常见的 QQ 攻击方式。

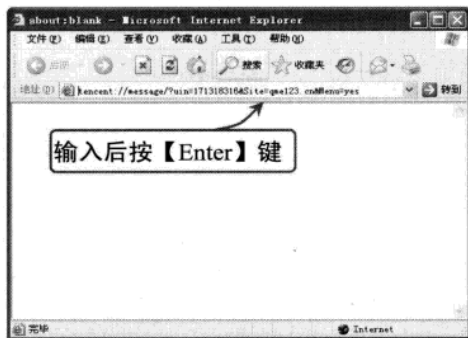
8.1.1 强制聊天

强制聊天是指在对方没有通过好友验证的情况下，强制打开聊天窗口。其主要原理是利用了 QQ 中的“临时对话”功能，通过命令代码强制建立“临时对话”窗口，即可进行聊天。

在已经登录 QQ 的状态下，打开浏览器，在地址栏中输入“tencent://message/?uin=*****&Site=qme123.cn&Menu=yes”（用想要强制聊天对象的 QQ 号代替****），按【Enter】键后，即强行打开临时对话窗口，具体操作步骤如下：

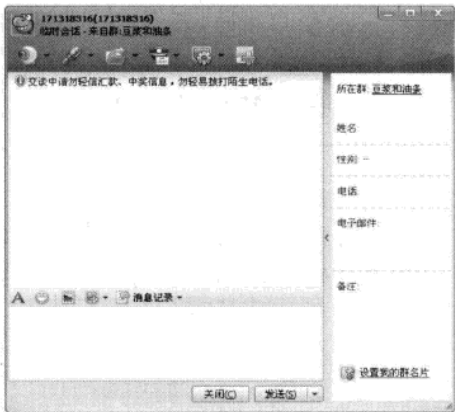
STEP 01 输入代码

打开 IE 浏览器，输入已经编写好的代码后，按【Enter】键确认，如下图所示。



STEP 02 强制聊天

在强制建立的“临时对话”窗口中，就可以对没有通过好友申请的另一 QQ 用户进行聊天了，如下图所示。



8.1.2 利用“炸弹”攻击

消息“炸弹”攻击可以说是“炸弹”攻击中最为常见的，它在瞬间向被攻击者发送大量垃圾信息从而造成网路堵塞，系统资源被大量占用，最后导致死机。“炸弹”攻击主要分为两种方式：向好友频繁发送信息和对陌生人频繁发送身份认证请求。

Work1 向好友频繁发送信息

QQ 消息“炸弹”原理其实比较简单：当用户打开聊天窗口时，QQ 消息“炸弹”程序通过调用函数等方式搜索到 QQ 聊天窗体及文本窗体等程序句柄，然后控制其自动发送垃圾信息。由于发消息时间间隔很短，使人应接不暇，最终形成了“炸弹”，导致被攻击者被迫退出 QQ 或重新启动计算机，其代表软件有“飘叶千夫指”，QQsend 等。

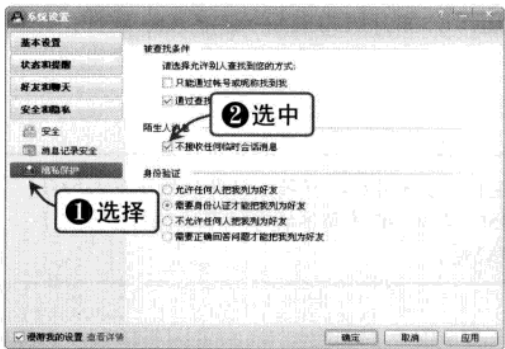
以上类型的攻击者都是通过了用户的验证，在用户的陌生人或好友名单中。我们可以通

Chapter 08 聊天软件攻防

过以下两种设置方法屏蔽掉陌生人或存于好友名单中的攻击者的消息，操作步骤如下：

STEP 01 不接收任何临时会话消息

在 QQ 的“系统设置”对话框中选择“安全和隐私”|“隐私保护”选项，在“陌生人消息”选项区中选中“不接收任何临时会话消息”复选框，这样就可以将陌生人的一切消息彻底地阻挡在外，如下图所示。



STEP 02 屏蔽好友中的攻击者消息

在 QQ 好友列表中选中攻击者并右击，在弹出的快捷菜单中选择“设置权限”|“屏蔽此人消息”选项即可，如下图所示。



Work2 频繁发送身份认证请求。

在 QQ “炸弹”中，还有一种身份认证“炸弹”，其代表软件有“QQ 砸门机”、“QQ 好友炸弹”等，就是利用 QQ 添加好友需要通过验证的步骤，向指定 QQ 号发送大量“身份认证”的请求信息。

当运行“砸门机”类的软件后，先输入自己的 QQ 号和要攻击的 QQ 号，然后再编辑发送请求的内容以及发送的次数。单击“开始”按钮，它就会成千上万次地向受害者的 QQ 发送请求“身份认证”的申请，让人不胜其烦！

当用户被 QQ 身份认证“炸弹”攻击时，最简单的处理方法就是立即通过认证，让攻击者成为你的“好友”，然后马上把他从好友名单拖到黑名单中。不过，这种方法也不是万能的，有经验的攻击者也会在他那边把你从他好友名单中删除，然后又以陌生人的身份再次进行身份认证的攻击。

8.1.3 破解本地 QQ 密码

当用户使用 QQ 时，会将账号、密码、好友列表、个人信息和聊天记录等经过数万次的 MD5 运算后，以加密文件的方式保存在本地电脑的 QQ 安装目录中，并且按照 QQ 安装目录分类。本地破解就是指盗号者通过技术手段破解 QQ 登录后保存在本地硬盘上的密码信息文件。

面对经过加密的 QQ 密码信息文件，大多数的破解软件都采用了相同的工作原理来破解，即穷举法。从理论上讲，只要穷举键盘上可以输入的所有字符串，就肯定能找到所需的 QQ 密码。破解软件采用穷举法来破解 QQ 密码，就是把密码中所有可能出现的字母或字符按照一定的算法进行排列组合，直到找到一组与密码完全匹配的字符序列。但是，这种方法



对于破解较复杂的密码时，由于组合数列过多，所以破解时间较长，有时会破解失败。

另一种方法是在获取了密码信息文件后，利用外挂“密码字典”来破解 QQ 密码的加密文件。所谓字典实际上是一个文本文件，里面包含有大量常用数字或字母的组合序列，也可以进行手动编辑。

我们要想防止密码破解软件对我们的密码进行暴力破解，首先要设置一个安全系数较高的密码，密码应当至少有 9 个字符长，不要以个人信息（如生日、名字等），不要以纯字母或纯数字形式出现。密码中要有一些非字母和非数字（如标点符号、控制字符等）的组合，如 Send20287591#&Add@%，这样的密码基本上是不可能被破解的。

其次，保护 QQ 密码安全还要提高自我安全意识，如升级为最新版本的 QQ 软件；在登录 QQ 时，取消选择登录界面中的“保存密码”复选框；定期更换 QQ 密码；在腾讯的官方网站及时申请密码保护等。



提示

所谓密码字典，主要是配合解密软件使用的，密码字典里包括许多人们习惯性设置的密码，比如生日、123456、ABCDE 等简单的有规律的密码，通过对照字典，能够大大提高密码的破解速度。

8.1.4 本地记录查询

QQ 的聊天记录中包含了很多个人信息，一旦被黑客盗取后用来进行网络诈骗，后果不堪设想。

当用户在系统登录 QQ 以后，就会在 QQ 安装目录生成一个该 QQ 号码的文件夹，里面以加密方式保存了该号码所有的配置信息、聊天记录等。但是，QQ 存在一个可以绕过密码在本地登录的漏洞。通过这个漏洞黑客可以绕远程系统的密码验证，从而突破 QQ 程序本身的限制，获取到记录在本地的信息内容。因此，无论在本地系统还是远程系统中，只需要获取到该目录中的文件即可。

如果要查询本地的记录，黑客只需要使用相关的黑客程序。运行该程序并选择任意一个已经登录过的 QQ 号码，则黑客程序就在系统后台中截取该 QQ 用户的所有聊天记录。

“赛博聊天记录监控器”是一款用于监控本机 QQ 聊天记录的软件，只要在本机登录过的 QQ，其聊天内容将被本软件监控。其具有以下特点：

- ❖ 绿色软件，真正免安装，解压缩后直接可以运行。
- ❖ 记录完整、整齐，包括可以显示在使用监控器以前的所有聊天记录。
- ❖ 主程序为单一文件，可任意改名，放在任何地方，隐蔽性高。

下面就以“赛博聊天记录监控器”为例，详细介绍类似软件的使用方法。

STEP 01 打开监控器

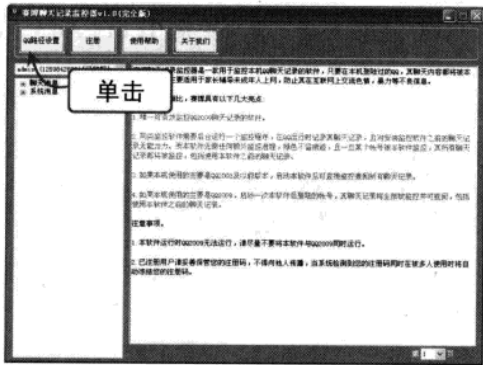
从网络上下载该软件后，运行软件，主界面如下图所示，单击“QQ 路径设置”按钮。

STEP 02 设置路径

弹出“路径选择”对话框，可以选中“手动设置路径”单选按钮。根据用户需要，选中“监控 QQ2008”单选按钮，单击“确定”按钮，如下图所示。

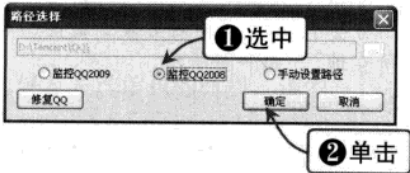
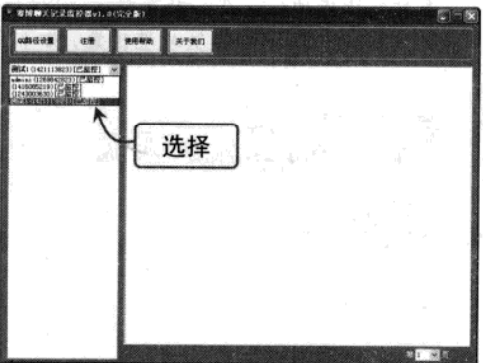
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 08 聊天软件攻防



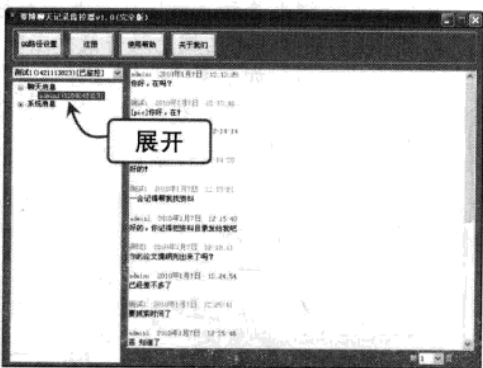
STEP 03 选择监控 QQ 号

在主界面的左窗格中单击下拉按钮，在弹出的下拉列表中选择要监控的 QQ 号码，如下图所示。



STEP 04 查看聊天记录

选中 QQ 号码后，分别显示了该 QQ 用户的聊天记录和消息记录。展开“聊天记录”分支，选择对话方后，主界面右窗栏则显示与该用户的所有聊天记录，如下图所示。



8.1.5 非法获取用户 IP

IP 是为计算机网络相互连接进行通信而设计的协议。在 Internet 中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在 Internet 上进行通信时应当遵守的规则。

IP 地址就是给每个连接在 Internet 上的主机分配的一个 32 位地址，其具有唯一性。当需要和一个 QQ 好友传输文件或者发送图片、表情时，QQ 软件必须知道对方的唯一 IP 地址和端口信息，这样才能把数据传给对方，即 QQ 内部已经实现了获取 IP 地址和其他信息的相关函数了。黑客就是通过指令函数来获取 IP 地址等相关信息，从而判断出对方的真实地理位置，或直接对获得的 IP 地址进行攻击。

目前比较常见的是在原版 QQ 的基础上加了显 IP 插件。下面以网上信念技术论坛开发的已安装显 IP 插件的 QQ 为例，介绍这个功能。

基础知识

与嗅探工具

Windows 系统漏洞攻防

安全策略

系统加密

远程攻击

木马

聊天软件

网页恶意

代码攻防

电子邮

攻击防

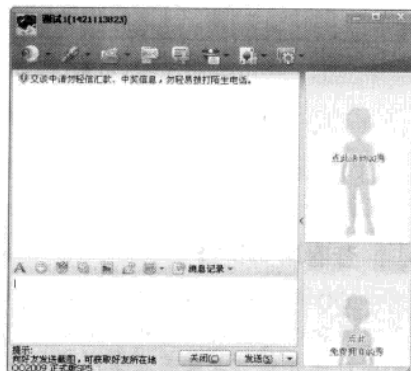
使用电脑

黑客攻防



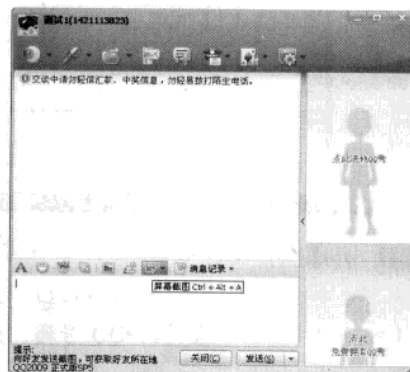
STEP 01 打开对话窗口

运行已经安装了显 IP 插件的 QQ 软件，双击要查看 IP 的好友名字，进入对话窗口，在窗口的下方会有提示：“向对方发送截图，可获得好友所在地”，如下图所示。



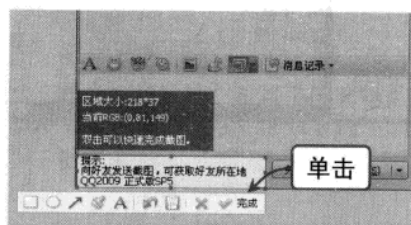
STEP 02 打开截图功能

在“好友对话”窗口中按【Ctrl+Alt+A】组合键，即可开启 QQ 截图功能，如下图所示



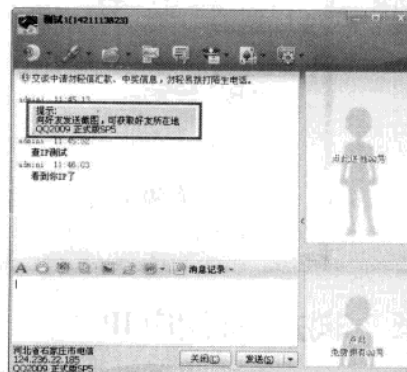
STEP 03 选择截图范围

按住鼠标左键并拖动，可以选择要截图的范围区域，在已经选定的区域上双击鼠标左键，单击“发送”按钮，如下图所示。当向对方发送截图图片后，后台插件软件开始获取 QQ 软件自身获得的 IP 地址。



STEP 04 显示 IP 和真实地理位置

图片发送成功后，在“好友对话”窗口下方就会显示对方的 IP 和真实地理位置，如下图所示。



8.1.6 QQ 尾巴病毒

下面将介绍 QQ 尾巴病毒的原理、主要特征以及清除 QQ 病毒的方法。

Work1 QQ 尾巴病毒的原理

QQ 尾巴病毒是一种木马病毒。它并不是利用 QQ 本身的漏洞进行传播，而是在某个网站首页上嵌入了一段恶意代码，利用 IE 浏览器的 iFrame 系统漏洞自动运行恶意木马程序，从而达到侵入用户系统，进而借助 QQ 进行垃圾信息发送的目的。

病毒在用户发送 QQ 消息时，先截获将要发送的正常消息，并在后面添加自己的恶意文字。病毒需要利用浏览器的漏洞欺骗用户单击网址，那么访问这些网站时其访问的网页中嵌

Chapter 08 聊天软件攻防

入的恶意代码即被运行。这些运行了的恶意程序会留在用户的系统中，自动监控 QQ 的聊天窗口、发送按钮等。当用户发送消息时它就将之截获，并在后面添加病毒自身指定的内容再发送出去，这样就形成了“QQ 尾巴”。

Work2 QQ 尾巴病毒的主要特征

QQ 尾巴病毒的主要特征是：当用户使用 QQ 向好友发送信息的时候，该木马程序会自动在发送的每一句消息末尾都插入一句诱骗用户单击的超链接，例如：

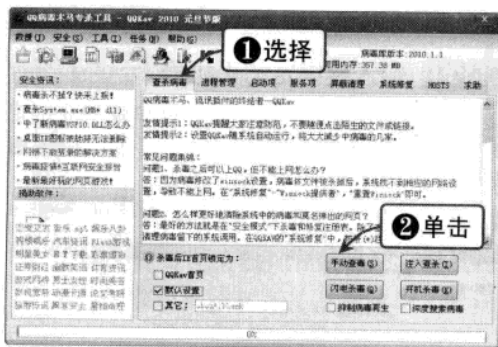
- ❖ 我的博客刚更新了新照片，去看看吧：http://photo***.126.com。
- ❖ 帮我个忙，看看这个网站能打开吗？http://www.tongyi***.com。
- ❖ 看看 http://www.hao***.com 最新的网络电影下载地址。
- ❖ 新年免费送 Q 币活动开始了！http://qq***.156.com。

Work3 QQ 尾巴病毒的清除方法

QQKav（QQ 病毒木马专杀工具）是一款专门查杀 QQ 尾巴病毒的专杀工具，用户可以利用它来进行清除。QQKav 是一款绿色软件，下载后可直接运行，无需安装。它能快速有效查杀各类 QQ 病毒及木马程序，及时清理流氓插件，遇到无法清除的顽固文件，还可以用“文件粉碎”功能来彻底清除，从而保护 QQ 的安全运行。下面将简单介绍其使用方法。

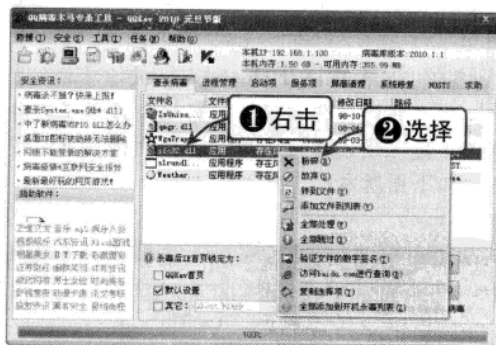
STEP 01 运行 QQKav

QQKav 下载完后可直接运行，在软件主界面上选择“查杀病毒”选项卡，单击“手动查杀”按钮，即开始对流行病毒和木马进行扫描，如下图所示。



STEP 02 扫描结果处理

扫描完后，会以列表形式显示扫描结果。对于 QQ 常见病毒和木马可直接进行清除，对于无法清除的文件，可以选中该文件后右击，在弹出的快捷菜单中选择“粉碎”选项，如下图所示。



8.2 保护好自己的 QQ

面对越来越多高超的黑客攻击手段，我们应该引起足够的重视来保护我们的 QQ 密码、聊天记录、资料信息等，及早地采取防护措施，除了平时养成定期修改密码并保证密码的复杂性等良好的习惯外，还可以通过 QQ 软件本身的特殊功能进行防御。

基础
知识

与嗅探
工具

统漏洞
攻防

安全策
略

系统
加密

远程
控制

攻
防

件攻
防

网
页

电
子

毒
攻

安
全

实
用

技
巧



8.2.1 设置 QQ 密码保护

QQ 密码保护是腾讯公司推出的保护用户 QQ 安全的一种方式，当用户的 QQ 密码发生问题无法登录时，可以通过填写正确的密码保护资料安全地取回密码。

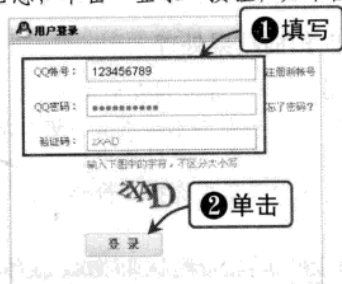
QQ 最新版本推出了密保手机、手机令牌、密保卡、密保问题四种密保手段，用户可以根据需要选择其中的一种或多种密保方法。下面将重点介绍密保手机和密保卡的绑定方法以及如何利用密码保护取回密码。

Work1 绑定密保手机

当我们把 QQ 绑定到一个常用的手机上时，就可以通过短信直接修改密码，并可以随时接受异常的修改密码通知，具体绑定方法如下：

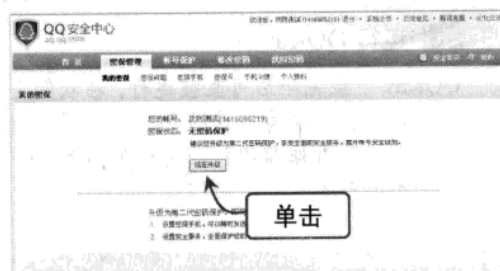
STEP 01 在 QQ 安全中心登录 QQ

在 IE 浏览器中输入 <http://aq.qq.com> 进入 QQ 安全中心，选择“密保管理”选项卡，在弹出的“用户登录”对话框中正确填写需要进行密码保护的“QQ 账号”、“QQ 密码”、“验证码”等信息，单击“登录”按钮，如下图所示。



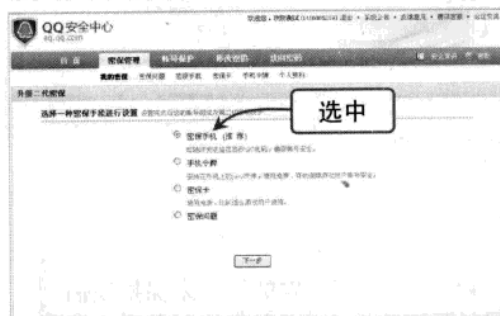
STEP 02 升级密码保护

在“我的密保”对话框中显示了该密码的密保状态，单击“现在升级”按钮，如下图所示。



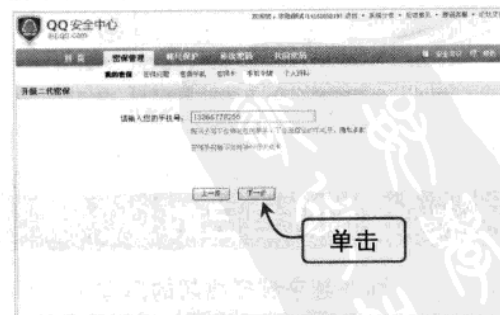
STEP 03 选择密保手段

在“升级二代密保”对话框中提供了四种密保手段可供选择，选中“密保手机”单选按钮，如下图所示。



STEP 04 输入要绑定的手机号码

在“升级二代密保”对话框中输入要绑定的手机号码，单击“下一步”按钮，如下图所示。



STEP 05 获取验证码

用绑定的手机根据提示发送短信，稍后验证码会以短信的方式返回。输入接收到的验证码，单击“下一步”按钮，如下图所示。

STEP 06 完成密保手机绑定

密保手机绑定成功，如需进行登录保护，可单击“设置 QQ 登录保护”按钮，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 08 聊天软件攻防

Work2 绑定密保卡

密保卡是二代密保中的一个密保手段，是一张记录着 10 行 8 列数字的卡片，可在 QQ 安全中心（<http://aq.qq.com>）中绑定。绑定成功后，用户可以通过验证密保卡坐标修改 QQ 密码、找回 QQ 账号、设置和使用安全服务等，具体绑定方法如下：

STEP 01 在 QQ 安全中心登录 QQ

在 IE 浏览器中输入 <http://aq.qq.com> 进入 QQ 安全中心，选择“密保管理”选项卡，在弹出的“用户登录”对话框中正确填写需要进行密码保护的“QQ 账号”、“QQ 密码”、“验证码”等信息，单击“登录”按钮，如下图所示。

STEP 02 升级密码保护

在“我的密保”对话框中，显示了该密码的密保状态，单击“现在升级”按钮，如下图所示。

STEP 03 选择密保手段

在“升级二代密保”的对话框中提供了四种密保手段可供选择，选中“密保卡”单选按钮，如下图所示。

STEP 04 领取密保卡

在“升级二代密保”的对话框中单击“领取一张保密卡”超链接，弹出“领取保密卡”对话框，单击“保存密保卡”按钮，即提示用户选择一个保存路径。并返回填写密保卡对话框，如下图所示。

序号	1	2	3	4	5	6	7	8
A	00	06	05	74	74	35	07	22
B	50	06	18	67	33	66	05	08
C	94	39	89	09	95	89	06	75
D	47	82	16	09	75	21	65	96
E	68	32	00	05	93	75	48	55
F	69	44	07	36	93	20	30	15
G	37	75	01	83	40	74	49	29
H	53	37	86	46	05	48	21	02
I	82	56	23	41	71	14	27	97
J	19	67	18	57	86	71	40	89

基础知识
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统与安全
件加密
远程控制
攻防
木马
聊天软件
网页恶意
代码攻防
件攻防
C 盘病毒
使用电脑
安全软件
黑客技巧

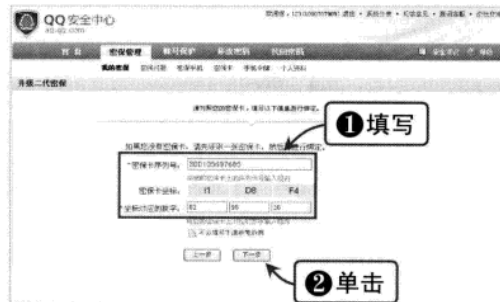
191

溜客安全网 WwW.176Ku.CoM



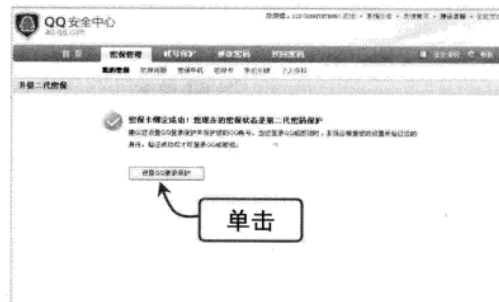
STEP 05 填写密保卡信息

对已经取得的密保卡，根据提示正确填写“密保卡序列号”、“坐标对应数字”等信息，单击“下一步”按钮，如下图所示。



STEP 06 完成密保卡绑定

提示密保卡绑定成功，如需进行登录保护，可单击“设置 QQ 登录保护”按钮，如下图所示（应注意妥善保管密保卡信息）。

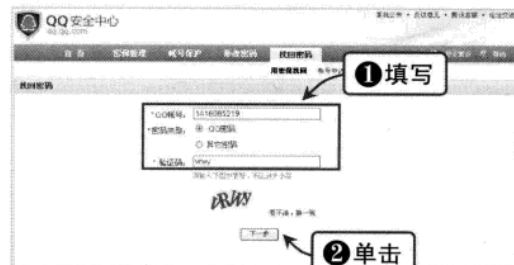


Work3 通过密码保护取回密码

用户的 QQ 申请了密码保护之后，在 QQ 密码发生问题时能够及时、安全地从 QQ 安全中心通过“取回密码”功能设置新的密码。

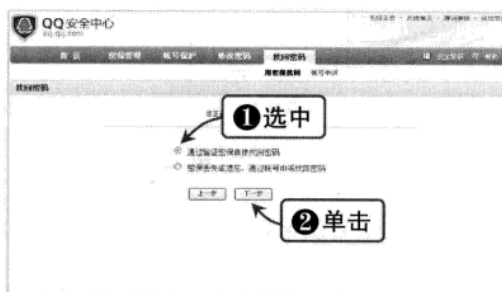
STEP 01 登录 QQ 安全中心

在 IE 浏览器中输入 <http://aq.qq.com> 进入 QQ 安全中心，选择“找回密码”选项卡，在弹出的对话框中正确填写需要找回密码的“QQ 账号”、“密码类型”、“验证码”等信息，单击“下一步”按钮，如下图所示。



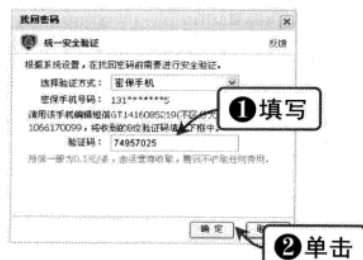
STEP 02 选择找回密码方式

在“找回密码”对话框中显示了要找回密码的 QQ 号，选中“通过验证密保直接找回密码”单选按钮，单击“下一步”按钮，如下图所示。



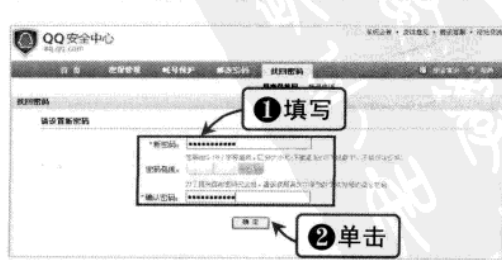
STEP 03 统一安全认证

在“升级二代密保”对话框中根据要求编写并发送短信，稍后验证码会以短信的方式返回。输入接收到的验证码，单击“确定”按钮。



STEP 04 输入新密码

验证通过后会弹出“请设置新密码”对话框，输入新密码，并确认新密码，单击“确定”按钮，即可重新设置 QQ 密码，如下图所示。



8.2.2 防范 IP 地址被探测

下面将介绍几种防范 IP 地址被探测的方法。

Work1 升级 QQ 软件

最新版本的 QQ 软件已经完成了 QQ 客户端的 IP 加密升级，好友将无法通过非法外挂来探测用户的 IP 地址以及地理位置。

Work2 限制文件传送

QQ 提供了在线传输文件的功能，部分攻击者就利用了这一特点，通过发送文件或图片的形式进行攻击探测，从而植入木马或病毒。因此，用户应加强在线传输的安全设置，不要随便接收陌生人发送的文件、图片等信息。已经接收到本地的文件也要经过杀毒软件的扫描方可运行。

Work3 安装防火墙

安装一个网络个人防火墙对于防御 IP 探测攻击也是很有必要的，如 ZoneAlarm 和天网等。如果在这些防火墙程序中将安全等级设置为“高”，它们就会对网络上发送和接收的每一个字节进行监测，同时也会对指定的端口进行实时查看，一旦发现有非正常的数据包企图进入计算机系统，它们就会加以拦截，并将发送方的 IP 地址与其他一些相关的信息提供给用户。这时，用户就能够根据数据包来源的 IP 地址判断是不是那些企图搞破坏的人所为，对 IP 地址扫描攻击程序起到很好的防护作用。

Work4 使用代理

当通过 ISP 服务商注册账号时，自己的计算机被分配了一个唯一的 IP 地址，这个地址被指定允许自己连接到 Internet 上。每次登录 QQ 时，用户的 IP 地址会被显示在中心服务器上。用户如果使用代理服务器，就可以隐藏自己的 IP 地址，让自己的踪迹从网络上消失。

首先，用户可以从网络上找到很多免费的代理服务器；其次，在 QQ 登录时进行代理服务设置。

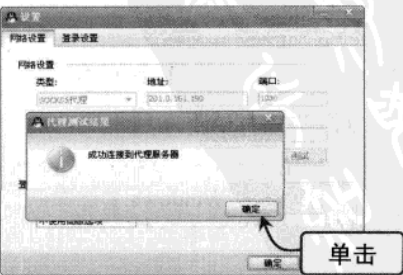
STEP 01 登录 QQ

在 QQ 登录的窗口中，单击“设置”按钮，如下图所示。



STEP 02 网络设置

在“设置”对话框中选择“网络设置”选项卡，选择代理服务器类型，输入代理服务器的地址和端口号，单击“测试”按钮。如果测试成功，在弹出的消息框中单击“确定”按钮，如下图所示。





8.2.3 利用“QQ 医生”保护 QQ 安全

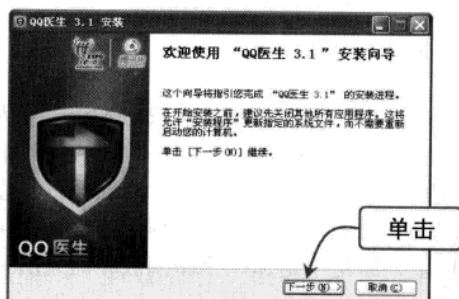
QQ 医生是腾讯公司开发的一款安全软件，不但可以有效地查杀 QQ 盗号木马，自动扫描系统漏洞和第三方软件漏洞，还提供了实用的系统工具。

Work1 QQ 医生的安装

用户应该到腾讯软件中心指定的 QQ 医生下载地址下载安装文件，下载地址为 <http://doctor.qq.com>。

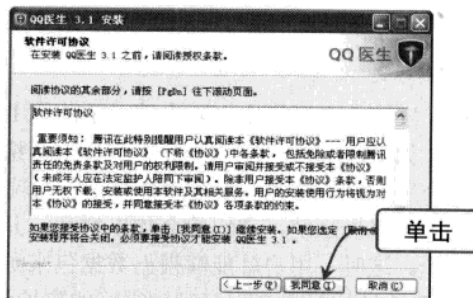
STEP 01 开始安装 QQ 医生

运行 QQ 医生安装程序，进入安装向导界面，单击“下一步”按钮，如下图所示。



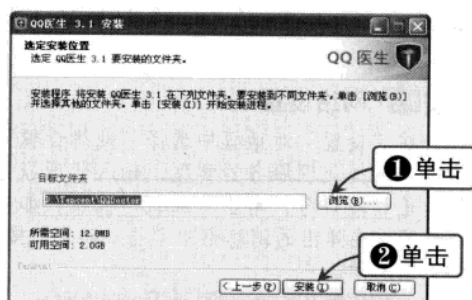
STEP 02 接受软件许可协议

阅读《软件许可协议》，单击“我同意”按钮，才可进行下一步安装，如下图所示。



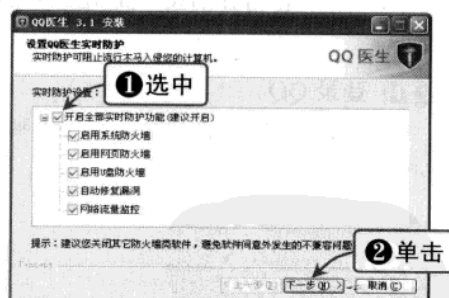
STEP 03 选择安装位置

单击“浏览”按钮，选择 QQ 医生的安装位置，单击“安装”按钮，如下图所示。



STEP 04 设置实时防护

开启 QQ 医生的实时防护功能，有效阻止流行木马的入侵。选中“开启全部实时防护功能”复选框，单击“下一步”按钮，直至完成，如下图所示。



Work2 QQ 医生的主要功能

QQ 医生具有以下几项主要功能：

- ❖ 全面扫描电脑风险，一键修复。
- ❖ 一键修复 Windows 系统漏洞，避免木马病毒利用漏洞攻击。
- ❖ 扫描木马病毒。

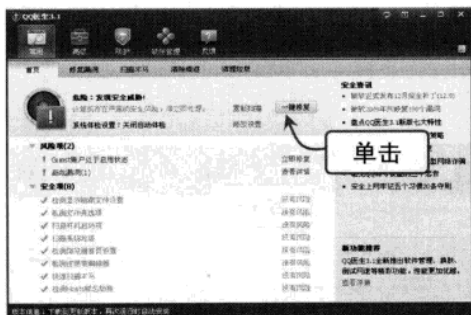
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 08 聊天软件攻防

- ❖ 清除计算机使用痕迹，保护个人隐私。
- ❖ 清理垃圾文件，节省空间，优化注册表，提高系统运行速度。
- ❖ 修复 IE 浏览器漏洞。
- ❖ 管理启动项，提高系统运行速度。
- ❖ 开启实时防御，阻断木马传播渠道。

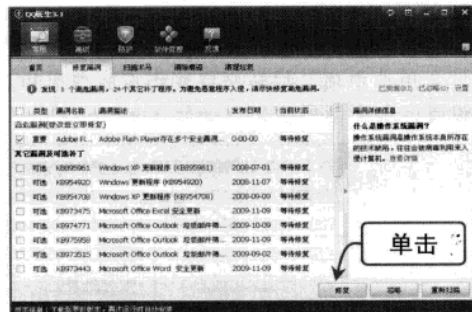
STEP 01 检测风险

在“QQ 医生”窗口中单击“常用”按钮，选择“首页”选项卡，单击“开始体检”按钮，即对用户计算机进行全面扫描。扫描结束后，在列表中显示需要修复的风险项，单击“一键修复”按钮进行修复，如下图所示。



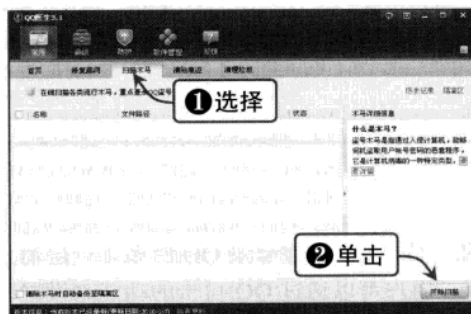
STEP 02 修复漏洞

选择“修复漏洞”选项卡，选择需要修复的系统漏洞，单击“修复”按钮，如下图所示。



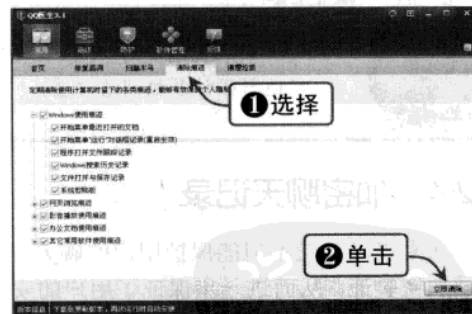
STEP 03 扫描木马

选择“扫描木马”选项卡，单击“开始扫描”按钮，即可扫描各种流行木马病毒，如下图所示。



STEP 04 清除痕迹

选择“清除痕迹”选项卡，选择列表中需要清除记录的复选框，单击“立刻清除”按钮，如下图所示。



STEP 05 清除垃圾

选择“清除垃圾”选项卡，选择列表中需要清除注册表垃圾的复选框，单击“立刻清除”按钮，如下图所示。

STEP 06 修复 IE 浏览器

在“QQ 医生”窗口中单击“高级”按钮，选择“修复 IE”选项卡。选择列表中需要修复的 IE 项目复选框，单击“立即修复”按钮，如下图所示。

黑客

常用扫描
与嗅探工具

漏洞扫描
系统漏洞扫描

安全策略
设置系统

系统安全
加密解密

远程控制
木马

聊天软件
代码攻防

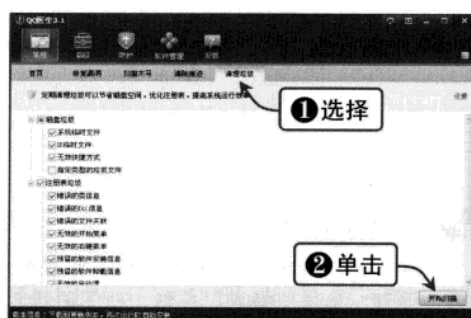
网页恶意
代码攻防

电子邮件
件攻防

C 语言
毒攻防

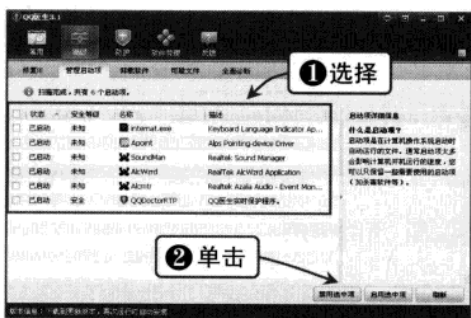
使用电脑
安全软件

黑客攻防
实用技巧



STEP 07 管理启动项

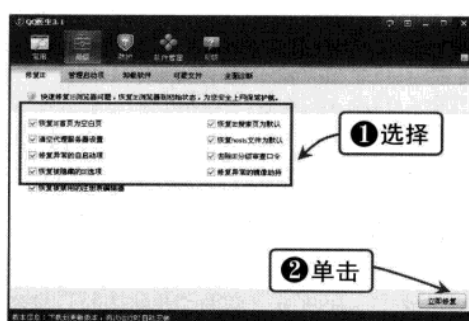
选择“管理启动项”选项卡，列表中列出了随用户计算机系统启动而自运行的文件。选择需要启动的文件名称后，单击“禁用选中项”或“启用选中项”按钮来完成相应的禁用和启动设置，如下图所示。



提示

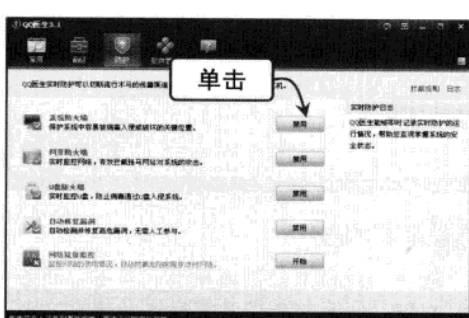


如果长期使用“QQ 医生”，建议用户打开所有的实时防护设置，这样能更好地增强计算机网络安全。



STEP 08 实时防护设置

在“QQ 医生”窗口中单击“防护”按钮，通过单击“禁用”或“开始”按钮关闭或开启各种防火墙和网络流量监控，如下图所示。



8.2.4 加密聊天记录

加密聊天记录不但能保护用户的聊天记录隐私不被偷窥，还在登录 QQ 时多了一层消息记录加密验证，从而进一步保证了用户的安全登录。用户可以通过 QQ 自带的功能来设置聊天记录的加密，操作方法如下：

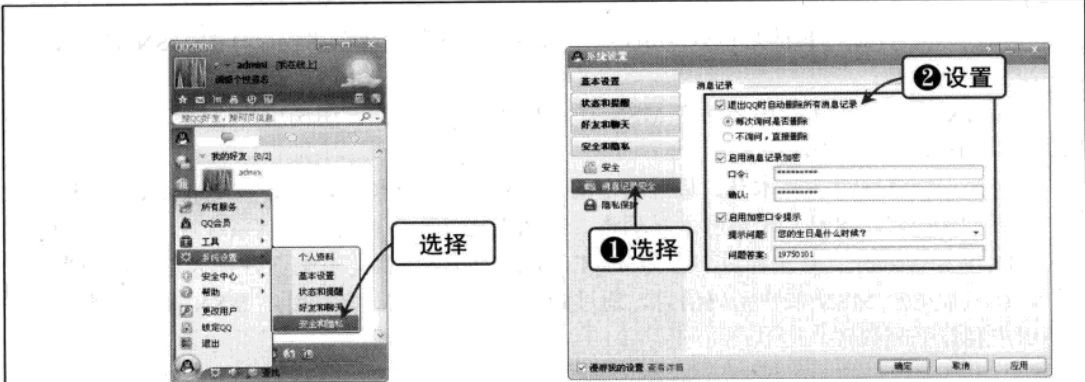
STEP 01 打开安全和隐私设置

在 QQ 主界面中选择“系统设置”|“安全和隐私”选项，如下图所示。

STEP 02 消息记录安全设置

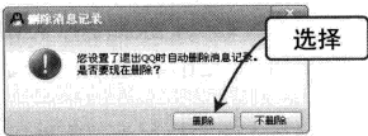
选择“消息记录安全”选项，选中“退出 QQ 时自动删除所有消息记录”复选框，选中“每次询问是否删除”单选按钮。选中“启用消息记录加密”复选框，输入加密口令。可通过选中“启用加密口令提示”复选框防止遗忘消息加密口令，如下图所示。

Chapter 08 聊天软件攻防



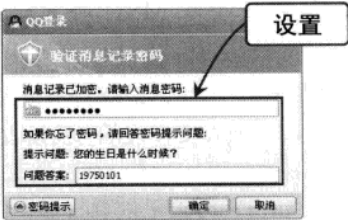
STEP 03 询问是否删除消息记录

在退出 QQ 软件时会出现提示信息框，用户可以根据需要选择是否删除所有的信息记录，如下图所示。



STEP 04 登录 QQ 提示

当再次登录 QQ 时，在输入 QQ 密码完后会出现要求输入消息密码的对话框，正确输入消息密码后，才能登录 QQ。如果忘记消息密码，正确填写提示问题答案，也可顺利登录 QQ，如下图所示。



8.3 MSN 的攻击与防御

MSN Messenger 是微软公司推出的即时通信软件，凭借其自身的优秀性能和简易操作，已跻身于目前世界上使用最为广泛的即时通信软件，在国内也有着众多的用户，这其中当然也包括大量企业用户。为了让企业内部员工，尤其是不同地区员工之间能良好的沟通又能节省通信费用，MSN Messenger 甚至被应用于跨国跨区贸易等商业交流。作为如此重要的信息交流工具，传输过程中的信息安全就尤为显得重要，下面就几种常见的方式，讲解针对 MSN 的攻击和防御知识。

8.3.1 针对 MSN 的攻击

MSN Messenger 作为重要的信息交流工具，成为攻击者的一个重要攻击目标。攻击者经常利用盗号木马盗取 MSN 账号，或者借助软件完整查看 MSN 的信息内容，如果内容中有重要信息，那后果将不堪设想。

Work1 MSN 盗号

MSN 账户是以电子邮件地址的形式存在的，只要知道了邮件地址和密码就可以进入到

黑客
基础知识和常用扫描工具
与嗅探工具
系统漏洞攻防
设置系统安全策略
系统与文件加密
远程控制
木马攻防
聊天软件攻防
网页恶意代码攻防
电子邮件攻防
C语言病毒
使用电脑安全软件
黑客攻防



相应账户。MSN 盗号指的是盗取 MSN 账户所对应的密码。现在比较流行的 MSN 盗号方式一般有以下两种：

一是使用网络钓鱼。黑客伪造 MSN 官方的登录网站页面，引诱用户进行账户登录，借此盗取 MSN 账号密码。

二是使用 MSN 盗号木马。最近流行的是“MSN 盗号木马变种 A (Trojan.PSW.Win32.MsnLiveTroj.a)”，这是一个盗号木马病毒，该病毒运行后将自身复制到系统目录中，在 C:\WINDOWS\system32 目录释放名称为 msnlive.exe 的病毒程序，并修改注册表选项，病毒运行后会记录用户 MSN 账户密码信息，通过邮件发送给黑客，窃取用户 MSN 账号、密码，使用户利益受到损害。



提示

网络钓鱼 (phishing)，黑客以种种名义引诱用户到其冒充的官方网站进行登录，盗取用户的账户密码等个人信息。这种伪造的网站以银行及电子商务等网站为主。

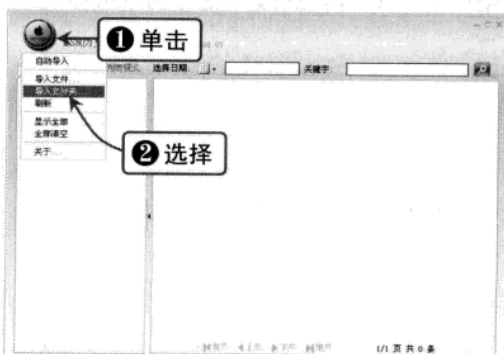
Work2 非法查看 MSN 聊天记录

MSN Messenger 的保密是基于 Windows 系统账户的，即使是使用同一台计算机，只要登录系统的账号不同，是查看不了 MSN 的聊天记录的。MSN 聊天记录都是以 XML 格式存放在相应账户个人文件夹的“我接收到的文件”目录下，如果别人用自己的账户登录计算机，就可以轻易地打开本地的 MSN 聊天记录进行查看。

使用“MSN 历史记录查看器”也可以非常轻松地对 MSN 聊天记录进行查看，具体操作步骤如下：

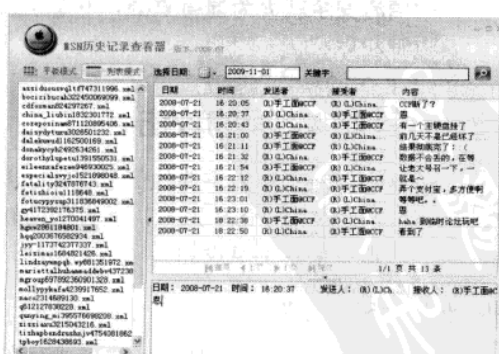
STEP 01 选择 MSN 历史记录存放位置

运行“MSN 历史记录查看器”程序，单击软件主界面左上角按钮，在弹出的菜单中选择“导入文件夹”选项，选择 MSN 历史消息的保存目录，单击“确定”按钮。软件会自动查找本地登录过的 MSN 账号，并对保存的相应聊天记录进行导入，如下图所示。



STEP 02 查看历史记录

历史记录导入完毕后，会在左窗格中显示本机 MSN 账户的好友列表。选择好友名称，将在右窗格中显示与该好友的所有聊天历史记录。也可通过选择日期和关键字的方法准确查找记录，如下图所示。



8.3.2 MSN 聊天加密

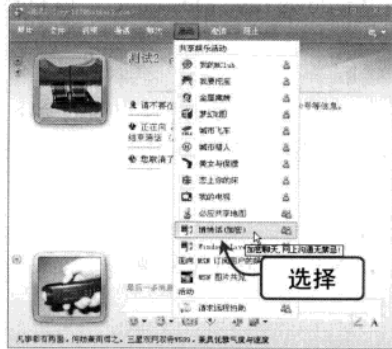
我们可以利用 MSN 中自带的“悄悄话”功能对用户的消息传输进行加密，防止网络传输过程中消息被截取，从而达到增强聊天安全性的目的。

Work1 使用“悄悄话”功能

使用“悄悄话”功能的具体操作方法如下：

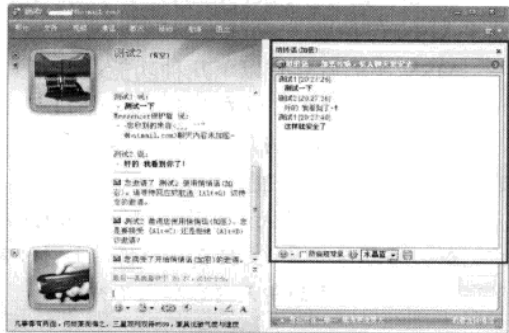
STEP 01 开启“悄悄话”功能

在 MSN 对话窗口中，选择“活动”|“悄悄话”选项，向对方发送一个“悄悄话”邀请申请，如下图所示。



STEP 02 进入“悄悄话”对话框

当对方接受了“悄悄话”的邀请，在对话窗口的右侧增加了一个“悄悄话”对话框，所有的聊天记录将被加密，如下图所示。



Work2 使用 Messenger Plus 加密 MSN 聊天记录

除了可以利用 MSN 本身的“悄悄话”功能进行聊天记录加密外，还可以借助第三方软件对 MSN 传输过程中的信息进行加密，这样就可以防止信息被攻击者获取，提高 MSN 信息传输的安全性。下面就以 Messenger Plus 为例，讲解它的加密聊天记录的功能。

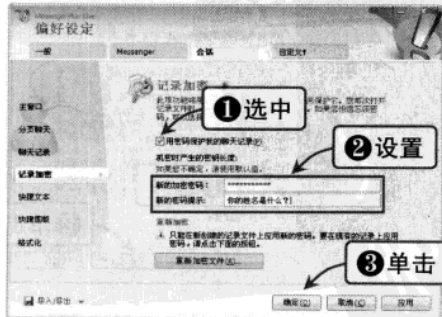
STEP 01 进入配置向导界面

进入 Messenger Plus 的官方网站 (<http://www.msgpluslive.net/?lang=zh-cn>)，单击相应的下载链接进行下载，并进行安装。安装完毕后进入“配置向导”对话框，单击“设定聊天记录加密”超链接，如下图所示。



STEP 02 “记录加密”设置

在“记录加密”选项区中选中“用密码保护我的聊天记录”复选框，并输入加密密码，同时设置新的密码提示问题，单击“确定”按钮即可，如下图所示。





8.3.3 Windows Live Messenger 保护盾

MSN 保护盾是一款由微软 MSN 和金山毒霸共同研发的 MSN 安全保护工具，专门针对中国市场的环境和特点而打造的即时通讯聊天安全辅助工具。

Work1 Windows Live Messenger 保护盾简介

MSN 保护盾 2.0 是微软 MSN 最新发布的 Messenger 安全增加工具，通过金山毒霸的“互联网可信认证”技术，帮助用户进行常规的 MSN 流行病毒检测和预防，实现更安全可靠的消息聊天。

MSN 保护盾会集成在 Windows Live Messenger 内，和 Windows Live Messenger 做到无缝整合。用户不需要特地去打开任何应用程序，因为在安装了 MSN 保护盾之后它就会植入到 Windows Live Messenger 的菜单中去。用户开启了 Windows Live Messenger，就自然地启动了 MSN 保护盾。

MSN 保护盾具有以下几种功能：

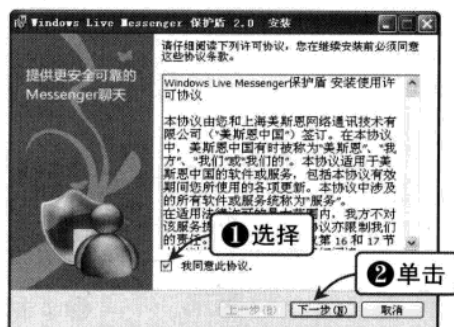
- ❖ 安全扫描：可以在 MSN 启动时进行安全扫描，也可为用户接收到的文件进行安全扫描。
- ❖ 加密聊天：当用户和好友都安装了保护盾 2.0 之后，彼此之间的聊天就会以密文方式传递，确保信息记录的完整、整齐；
- ❖ 屏蔽恶意骚扰：屏蔽攻击者发来的恶意骚扰信息；
- ❖ 多账号登录：支持在一台机器上同时登录多个 MSN 账号。在安全实现无缝切换的同时，保证不同账号之间的聊天内容独立不冲突。

Work2 使用 Windows Live Messenger 保护盾

用户可以到 Windows Live Messenger 保护盾的官方网站（<http://im.live.cn/safe>）下载最新版本 Windows Live Messenger 保护盾软件。下面将简单介绍其安装方法和安全设置。

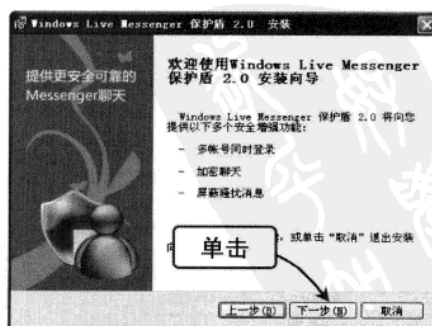
STEP 01 运行 Messenger 保护盾安装程序

在官方网站上下载最新版本 Messenger 保护盾软件。文件下载完毕后，双击其安装程序图标，运行安装程序，阅读《Windows Live Messenger 保护盾安装许可协议》，选中“我同意此协议。”复选框，如下图所示。



STEP 02 使用安装向导

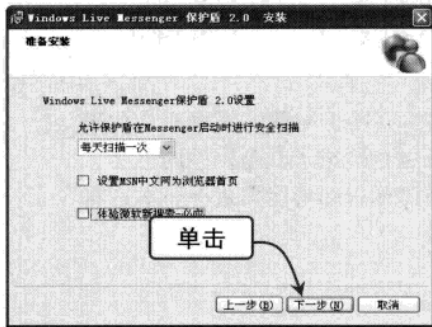
进入 Windows Live Messenger 保护盾安装向导，单击“下一步”按钮继续安装，如下图所示。



Chapter 08 聊天软件攻防

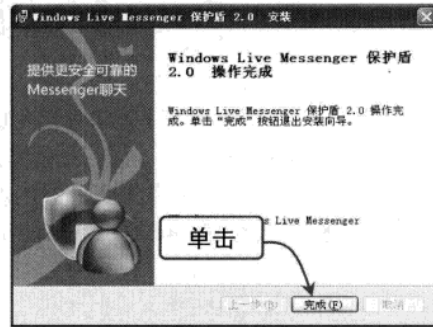
STEP 03 Messenger 保护盾设置

在此对话框设置中启动安全扫描，并设置安全扫描的频率，单击“下一步”按钮，如下图所示。



STEP 04 完成 Messenger 保护盾安装

安装完成后，单击“确定”按钮完成安装，如下图所示。



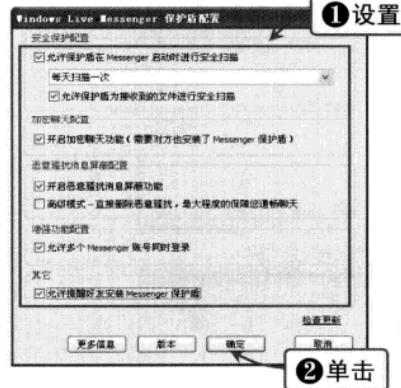
STEP 05 内存病毒扫描

在 MSN 主界面上选择“显示菜单”|“工具”|“Messenger 保护盾配置”选项，初次进入后，自动进行内存病毒扫描，如下图所示。



STEP 06 Messenger 保护盾配置

在“Windows Live Messenger 保护盾配置”对话框中，用户可根据需要开启各种功能设置，单击“确定”按钮，如下图所示。



黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
件攻防
网页恶意
代码攻防
电子邮箱
C 盘病毒
使用电脑
黑客攻防
实用技巧

Chapter

09

网页恶意代码攻防

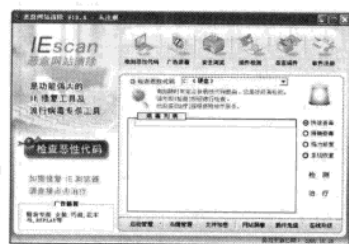
如今广大网民最讨厌和最害怕的是什么？莫过于所谓的网页恶意代码了。在网上稍不留神，就会发现自己的 IE 标题栏换成了其他网站的名字、默认主页被篡改、系统注册表被禁用、IE 中鼠标右键功能失效……本章将详细介绍网页恶意代码的攻击与防护知识。

本章建议学习时间：

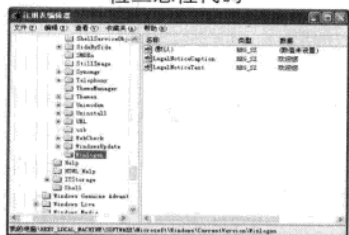
本章建议学习时间为 60 分钟，其中分配 35 分钟学习网页恶意代码攻防的相关知识，25 分钟观看教学视频和课件并进行练习。

学完本章后您可以：

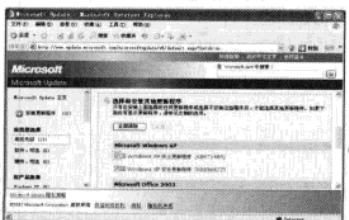
- 了解恶意代码的相关信息
- 学会恶意代码的预防和清除
- 常见恶意代码及解决方法
- IE 浏览器常用设置
- 用“360 安全卫士”修复 IE 浏览器
- 使用“瑞星卡卡上网助手”



检查恶性代码



针对弹出对话框现象



系统更新

重要知识点视频索引



9.1 恶意代码简介

电脑用户在上网时经常会遇到偷偷篡改 IE 标题栏的网页代码，有的网站更是不择手段，当用户访问过它们的网页后，不仅 IE 默认首页被篡改了，而且每次开机后 IE 都会自动弹出并访问该网站。以上这些情况都是因为感染了网络上的恶意代码。

9.1.1 恶意代码概述

恶意代码最常见的表现形式就是网页恶意代码。网页恶意代码的技术以 WSH 为基础，即 Windows Scripting Host，中文称做“Windows 脚本宿主”。它是利用网页来进行破坏的病毒，使用一些用 Script 语言编写的恶意代码，利用 IE 的漏洞来实现病毒植入。

当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以对用户的电脑系统进行破坏，强行修改用户操作系统的注册表配置及系统实用配置程序，甚至可以非法控制被攻击电脑的系统资源、盗取用户文件、删除硬盘中的文件、格式化硬盘等。

9.1.2 WSH 知识

下面将介绍有关 WSH 概念、作用、工作流程方面的知识。

Work1 WSH 简介

WSH，是 Windows Scripting Host 的缩写形式，其通用的中文译名为“Windows 脚本宿主”。对于这个较为抽象的名词，可以作这样一个笼统的理解：它是内嵌于 Windows 操作系统中的脚本语言工作环境。

Windows Scripting Host 这个概念最早出现于 Windows 98 操作系统。大家一定还记得 MS-DOS 下的批处理命令，它有效地简化了工作，这类似于如今的脚本语言。但就算把批处理命令看成是一种脚本语言，那它也是 98 版之前的 Windows 操作系统所唯一支持的“脚本语言”。而此后随着各种真正的脚本语言不断出现，批处理命令显然就力不从心了。面对这一危机，微软在研发 Windows 98 时，为了实现多类脚本文件在 Windows 界面或 DOS 命令提示符下的直接运行，就在系统内植入了一个基于 32 位 Windows 平台、并独立于语言的脚本运行环境，并将其命名为 Windows Scripting Host。WSH 架构于 ActiveX 之上，充当 ActiveX 的脚本引擎控制器，WSH 为 Windows 用户充分利用威力强大的脚本指令语言扫清了障碍。

WSH 诞生后，在 Windows 系列产品中很快得到了推广。除了 Windows 98 之外，微软在之后研发的操作系统中都嵌入了 WSH。

Work2 WSH 的作用

WSH 的设计，在很大程度上考虑到了“非交互性脚本（noninteractive scripting）”的需要。在这一指导思想下产生的 WSH，给脚本带来非常强大的功能，例如，可以利用它完成映射网络驱动器、检索及修改环境变量、处理注册表项等工作；管理员还可以使用 WSH 的

- 基础知 黑客
- 与嗅探工具 常用扫描
- 统漏洞攻防 Windows 系
- 安全策略 设置系统
- 件加密 系统与文
- 制攻防 远程控
- 攻防 木马
- 件攻防 聊天软
- 代码攻防 网页恶
- 件攻防 电子邮
- 毒攻防 C 盘病
- 安全软件 使用电
- 实用技巧 黑客攻



支持功能来创建简单的登录脚本，甚至可以编写脚本来管理活动目录。

Work3 WSH 工作流程

WSH 的工作流程，实际上就是脚本文件被解析并执行的过程。我们知道，现在脚本经常会被植入网页，其中包括 HTML 页面（客户端）和 ASP 页面（服务器端）。对于植入 HTML 页面的脚本，其所需的解析引擎会由 IE 这样的网页浏览器载入；对于植入 ASP 页面的脚本，其所需的解析引擎会由 IIS（Internet Information Services）提供。

而对于出现在 HTML 和 ASP 页面之外的脚本（它们常以独立的文件形式存在），就需要经由 WSH 来处理了。WSH 正常工作的前提是用户必须安装了微软 3.0 或更高版本的 IE，因为 WSH 在工作时会调用 IE 中的 VBScript 和 JScript 解析引擎。

WSH 根据脚本文件后缀名，到系统注册表中查询所需的脚本引擎。VBScript 和 JScript 两种语言的解析引擎是 Windows 系统中原有的，而其他脚本语言的解析引擎，如 PERL、TCL 等，需要用户另行定义；执行脚本命令时，一些脚本指令会使用到 WSH 内置对象所提供的服务，如处理注册表项。这时，脚本指令就会向 WSH 提出请求，并由 WSH 完成所需任务。也正是在这一步，WSH 的功用得到了淋漓尽致的发挥。

9.1.3 恶意代码的特征

恶意代码（malicious code）或者叫恶意软件（malicious software）具有以下共同特征：

- ❖ 恶意的目的。
- ❖ 本身是程序。
- ❖ 通过执行发生作用。

有些恶作剧程序或者游戏程序不能看作是恶意代码。对过滤性病毒的特征进行讨论的文献很多，尽管它们数量很多，但是机理比较近似，在防病毒程序的防护范围之内，更值得注意的是非过滤性病毒。

9.1.4 非过滤性病毒

非过滤性病毒包括口令破解软件、嗅探器软件、键盘输入记录软件，远程特洛伊和间谍等，组织内部或者外部的攻击者使用这些软件来获取口令、侦察网络通信、记录私人通信、暗地接收和传递远程主机的非授权命令，而有些私自安装的 P2P 软件实际上等于在企业的防火墙上开了一个口子。非过滤性病毒有逐年增长的趋势，电脑用户要加强对它的防御。

9.1.5 恶意代码的传播方式

恶意代码的传播方式在迅速地演化，从引导区传播，到某种类型文件传播，到宏病毒传播，到邮件传播，再到网络传播，发作和流行的时间越来越短，危害越来越大。

目前，恶意代码主要通过网页浏览或下载、电子邮件、局域网和移动存储介质、即时通讯工具（IM）等方式传播。广大电脑用户遇到的最常见的方式是通过网页浏览方式进行攻击，这种方式具有传播范围广、隐蔽性较强等特点，潜在的危害性也是最大的。

9.2 恶意代码的预防和清除

虽然有的恶意代码的破坏性不是很大，但是恶意代码常常对用户电脑系统做一些强制设置，并且清除起来非常麻烦。因此，电脑用户要学会对恶意代码的预防和清除。

9.2.1 恶意代码的预防

电脑用户在上网前和上网时做好如下工作，才能对网页恶意代码进行很好的预防：

- ❖ 要避免被网页恶意代码感染，首先关键是要不要去一些自己并不了解的站点，尤其是一些看上去非常美丽诱人的网址更不要轻易进入，否则往往不经意间就会误入网页代码的圈套。
- ❖ 微软官方经常发布一些漏洞补丁，要及时对当前操作系统及 IE 浏览器进行更新升级，可以更好地对恶意代码进行预防。
- ❖ 一定要在电脑上安装病毒防火墙和网络防火墙，并要时刻打开“实时监控功能”。通常防火墙软件都内置了大量查杀 VBS、JavaScript 恶意代码的特征库，能够有效地警示、查杀、隔离含有恶意代码的网页。
- ❖ 对防火墙等安全类软件进行定时升级，并在升级后检查系统进程，及时了解系统运行情况。定期扫描系统（包括病毒扫描与安全漏洞扫描），以确保系统安全。
- ❖ 关闭局域网内系统的网络硬盘共享功能，防止一台电脑中毒影响到网络内的其他电脑。
- ❖ 利用 hosts 文件可以将已知的广告服务器重定向到无广告的机器（通常是本地的 IP 地址，如 127.0.0.1）上来过滤广告，从而拦截一些恶意网站的请求，防止访问欺诈网站或感染一些病毒或恶意软件。
- ❖ 对 IE 浏览器进行详细安全设置。



提示

hosts 文件是一个用于储存电脑网络中各结点信息的电脑文件。这个文件负责将主机名映射到相应的 IP 地址。hosts 文件可以用记事本直接进行编辑，通常用于补充或取代网络中 DNS 的功能。hosts 文件在 Windows NT/2000/XP/2003/Vista 操作系统中的默认位置为 Windows\system32\drivers\etc\。

9.2.2 恶意代码的清除

即便是电脑感染了恶意代码，也不要着急，只要用户按照正确的操作方法是可以使系统恢复正常的。如果用户是个电脑高手，就可以对注册表进行手工操作，使被恶意代码破坏更改的地方恢复正常。对于普通的电脑用户来说，就需要使用一些专用工具来进行清除。

Work1 使用 IEScan 恶意网站清除软件

IEScan 恶意网站清除软件是功能强大的 IE 修复工具及流行病毒专杀工具，它可以进行恶意代码的查杀，并可免疫常见的恶意网络插件。

基础知识

常用扫描
与嗅探工具

系统漏洞
安全策略

设置系统
安全策略

系统与文
件加密

远程控制
制攻防

木马
攻防

聊天软
件攻防

网页恶
意代码防

电子邮
件攻防

使用电
脑安全软

黑客攻
防实用技

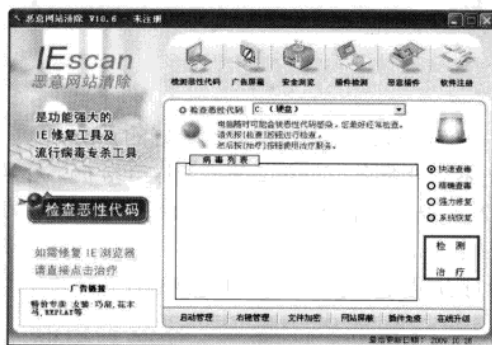
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



黑客攻防从新手到高手

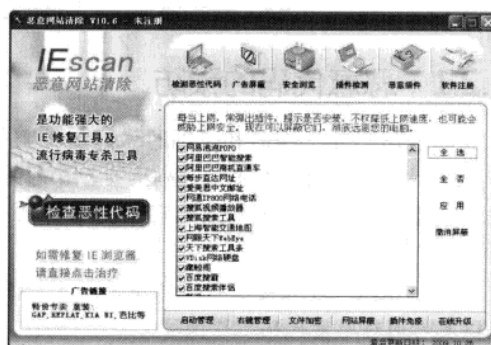
STEP 01 检查恶性代码

运行 IEScan 恶意网站清除软件，单击“检测”按钮，可以对电脑系统进行恶意代码的检查。直接单击“治疗”按钮，则可以对 IE 浏览器进行修复，如下图所示。



STEP 02 插件免疫

单击“插件免疫”按钮，显示软件窗口，以列表形式显示了已知的恶意插件的名称，选中对应的复选框，单击“应用”按钮，如下图所示。

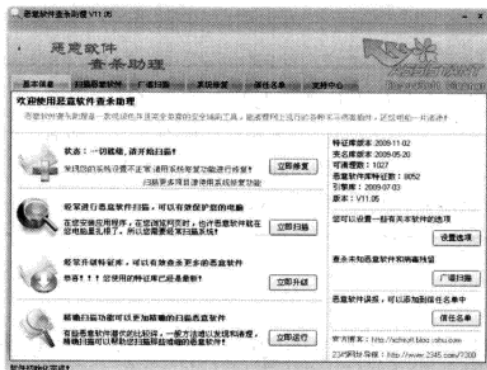


Work2 使用恶意软件查杀助理

恶意软件查杀助理是针对目前网上流行的各种木马病毒以及恶意软件开发的。恶意软件查杀助理可以查杀超过 900 多款恶意软件、木马病毒插件，找出隐匿在系统中的有害程序。具体使用方法如下：

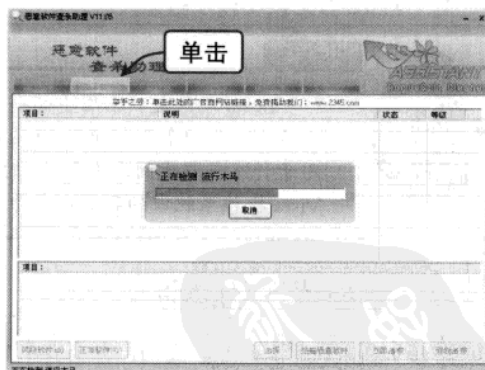
STEP 01 运行恶意软件查杀助理

安装软件后，单击桌面上的恶意软件查杀助理程序图标，启动恶意软件查杀助理，其主界面如下图所示。



STEP 02 扫描恶意软件

单击“扫描恶意软件”按钮，软件开始检测电脑系统，如下图所示。



STEP 03 运行恶意软件查杀工具

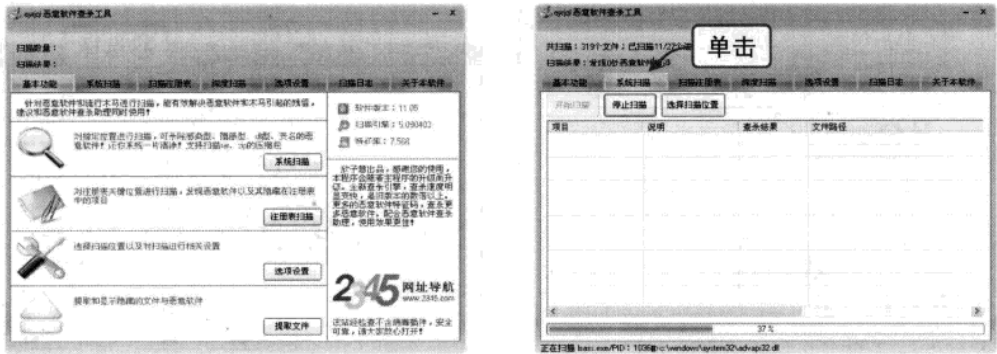
在恶意软件查杀助理安装的同时，还要安装一个恶意软件查杀工具。运行恶意软件查杀工具，主界面如下图所示。

STEP 04 系统扫描

单击“系统扫描”按钮，软件开始对电脑系统进行扫描，并实时显示扫描过程，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 09 网页恶意代码攻防



提示



“系统扫描”完成后，用户可以根据软件提示的结果进行进一步的清除操作。因此，一定要记得经常对电脑系统进行系统扫描。

9.3 常见恶意代码及解决方法

网络上的恶意代码各种各样，怎样判断电脑是否已经感染恶意代码呢？如果已经感染恶意代码，又怎样进行清除呢？下面总结了几种最常见的恶意代码及相应的解决方法。

9.3.1 启动时自动弹出对话框和网页

相信大多数用户都会遇到下面的情况：

- ❖ 系统启动时弹出对话框，通常是一些广告信息，如“欢迎访问某某网站”等。
- ❖ 开机弹出网页，通常会弹出很多窗口，让你措手不及，更有甚者，可以重复弹出窗口直到死机。

这就说明恶意代码修改了用户的注册表信息，使得启动浏览器时出现异常。可以通过编辑系统注册表来解决，具体操作步骤如下：

STEP 01 针对弹出对话框现象

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令。打开注册表编辑器，打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon 主键，删除右窗格中的 LegalNoticeCaption 和 LegalNoticeText 两个字符串，如下图所示。

STEP 02 针对弹出网页现象

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 msconfig 命令，选择“启动”选项卡，如下图所示。把列表中后缀名为 url、html、htm 的网址文件前的复选框都选中，单击“应用”按钮。

基础知识

常用扫描与嗅探工具

统漏洞攻防

设置系统安全策略

系统与文件加密

远程攻击

木马攻击

聊天软件攻击

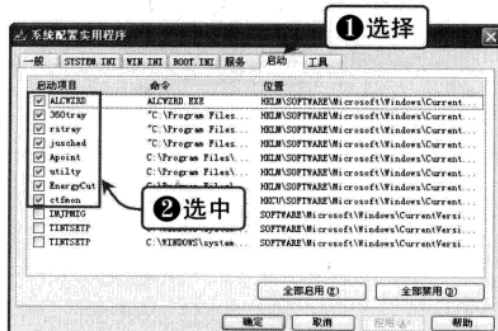
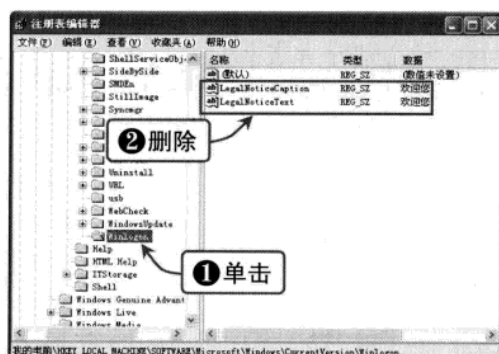
网页恶意代码攻防

电子邮件攻击

C盘病毒

使用电脑安全软件

黑客攻防实用技巧



9.3.2 修改起始页和默认主页

某些网站为了提高自己的访问量和做广告宣传，就使用恶意代码，利用 IE 浏览器的漏洞，将访问者的 IE 浏览器不由分说地进行修改。一般改掉 IE 浏览器的起始页和默认主页。用户可以通过编辑系统注册表来解决，具体操作步骤如下：

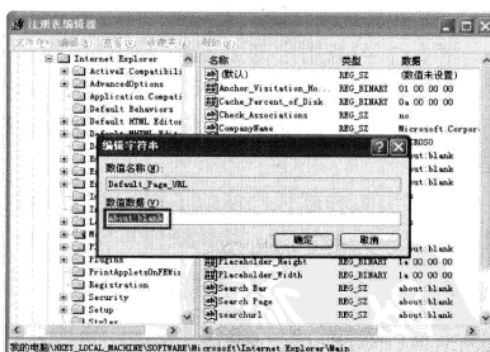
STEP 01 针对起始页的修改

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令。打开注册表编辑器，打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Internet Explorer\Main 主键，在右窗格中将 StartPage 子键的键值改为 about:blank 即可，如下图所示。同时，还要将注册表 HKEY_CURRENT_USER 下的相同位置做同样操作。



STEP 02 针对默认主页的修改

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令。打开注册表编辑器，打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Internet Explorer\Main 主键，在右窗格中将 Default_Page_URL 子键的键值中的那些恶意网站的网址改正，或者设置为 IE 的默认值，如下图所示。



9.3.3 强行修改 IE 标题栏

在系统默认状态下，由应用程序本身来提供标题栏的信息，但也允许用户自行在上述注册表项目中添加信息，一些恶意代码强制更改用户的 IE 浏览器标题栏的内容，强迫用户观看一些地址或广告。

Chapter 09 网页恶意代码攻防

用户可以通过编辑系统注册表来解决，具体操作步骤如下：

STEP 01 删除 Window Title 串值

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令。打开注册表编辑器。打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Internet Explorer\Main 主键，在右窗格中将 Window Title 串值删除。如下图所示。同时，还要在注册表 HKEY_CURRENT_USER 下的相同位置做同样操作。



STEP 02 更改 Window Title 串值

或双击 Window Title 串值，弹出“编辑字符串”对话框，把“数值数据”改为 Microsoft Internet Explorer，IE 浏览器就可以恢复正常状态，如下图所示。同时，还要在注册表 HKEY_CURRENT_USER 下的相同位置做同样操作。



提示



通过 Regedit 注册表编辑器手工对 Windows 系统注册表进行修改的操作方法非常实用，读者一定要掌握，在今后的工作、学习和生活中可能会经常用到。

9.3.4 强行修改右键菜单

被强行修改右键菜单的现象主要表现在：

- ❖ 右键快捷菜单被添加非法网站链接；
- ❖ 右键弹出快捷菜单功能被禁用失常，在 IE 浏览器中右击无反应。

以上问题用户可以通过编辑系统注册表来解决，具体操作步骤如下：

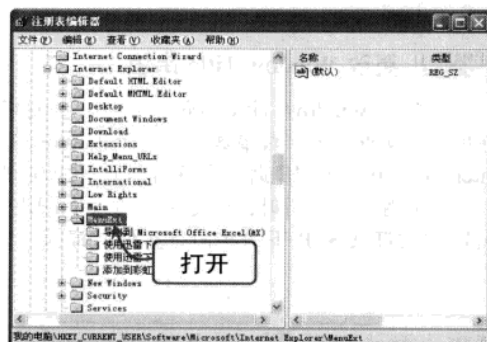
STEP 01 删除注册表广告链接

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令，打开注册表编辑器。打开 HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt 主键，在右窗格中删除相关的广告条文，如下图所示。

STEP 02 恢复右键功能

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令，打开注册表编辑器。打开 HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions 主键，将其 NoBrowserContextMenuDWord 值改为 0，如下图所示。

黑客
常用扫描
漏洞探测工具
系统漏洞攻防
设置系统
安全策略
系统与安全
加密
远程控制
木马
聊天软件
网页恶意
代码攻防
电子邮件
C 漏洞
使用电脑
黑客攻防



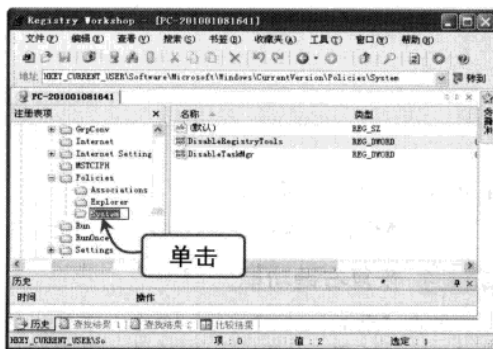
9.3.5 禁用注册表

有时浏览了恶意网页后系统被修改，想要用 Regedit 注册表编辑器更改时，却发现系统提示没有权限运行该程序，无法运行。这说明恶意代码不但修改了我们的浏览器设置，甚至禁用了注册表编辑功能。

遇到这种情况，用户可以从网上下载一个第三方的注册表编辑器，推荐使用 Registry Workshop 软件。Registry Workshop 是一款高级的注册表编辑工具，能够完全替代 Windows 系统自带的注册表编辑器，官方网站地址为 <http://www.torchsoft.com/>。具体使用方法如下：

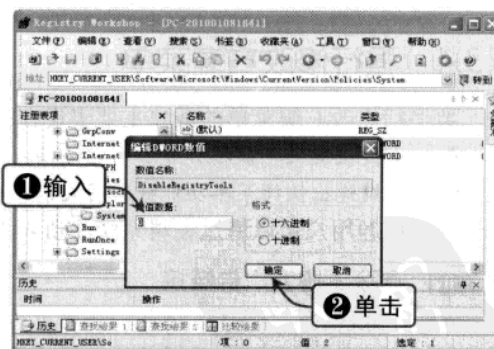
STEP 01 打开 System 主键

下载 Registry Workshop 软件后，安装运行。使用方法和系统注册表编辑器基本一致。在软件左窗格中打开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 主键，如下图所示。



STEP 02 编辑 DWORD 数值

在右窗格中把 DisableRegistryTools DWORD 值的“数值数据”改为 0。单击“确定”按钮，并退出 Registry Workshop 软件，重新启动电脑，即可恢复注册表的系统权限，如下图所示。



9.4 IE 浏览器安全维护

网络上的恶意代码往往是在 IE 浏览器浏览网页时激发的，用户可以对 IE 浏览器进行安全设置，并使用相关安全软件进行安全防护。

9.4.1 IE 浏览器安全设置

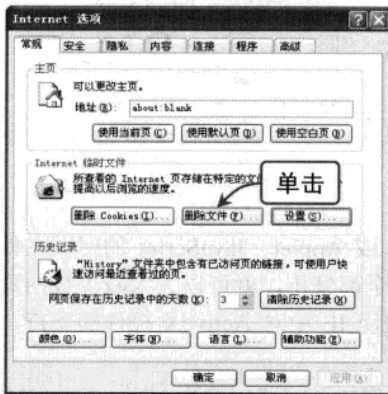
下面将介绍 IE 浏览器安全设置方面的知识，读者应该熟练掌握。

Work1 清除 IE 浏览器各项内容

通过以下设置可以对 IE 浏览器的临时文件、Cookies、访问历史记录、自动完成信息等内容进行清除，具体操作步骤如下：

STEP 01 打开“Internet 选项”对话框

运行 IE 浏览器，单击“工具”|“Internet 选项”命令，打开“Internet 选项”对话框，如下图所示。单击“Internet 临时文件”选项区中的“删除文件”按钮。



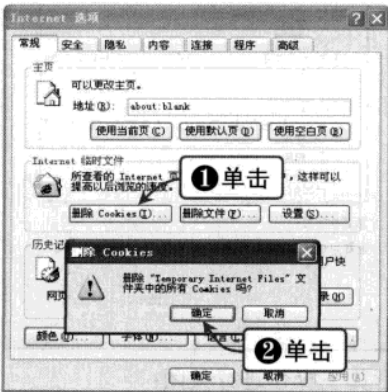
STEP 02 清除 IE 浏览器中的临时文件

弹出“删除文件”提示信息框，选中“删除所有脱机内容”复选框，单击“确定”按钮，对 IE 浏览器的临时文件进行清除，如下图所示。



STEP 03 清除 IE 浏览器中的 Cookies

在“Internet 选项”对话框中，单击“Internet 临时文件”选项区的“删除 Cookies”按钮，弹出“删除 Cookies”提示信息框，单击“确定”按钮即可，如下图所示。



STEP 04 清除 IE 浏览器的历史记录

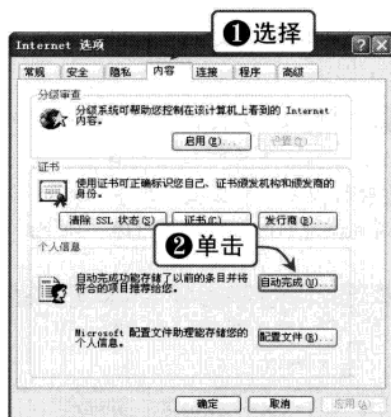
在“Internet 选项”对话框中，单击“历史记录”选项区的“清除历史记录”按钮，弹出“Internet 选项”提示信息框，单击“是”按钮，即可完成对已访问的历史记录的清除，如下图所示。





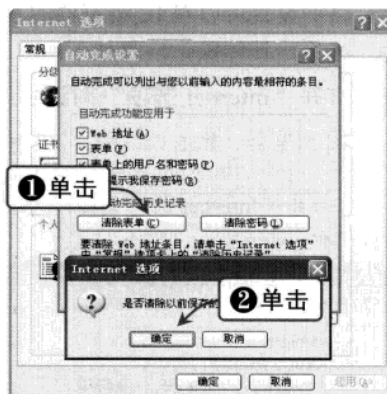
STEP 05 选择“内容”选项卡

在“Internet 选项”对话框中选择“内容”选项卡，单击“个人信息”选项区中的“自动完成”按钮，如下图所示。



STEP 06 清除表单

弹出“自动完成设置”对话框，单击“清除表单”按钮，弹出“Internet 选项”提示信息框，单击“确定”按钮，清除 IE 浏览器自动保存的条目内容，如下图所示。

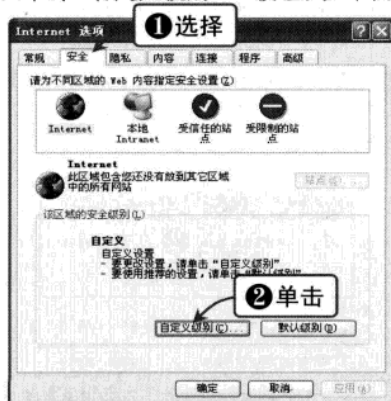


Work2 IE 浏览器的 ActiveX 控件设置

因为这一类网页主要是含有恶意代码的 ActiveX 或 Applet、JavaScript 的网页文件，所以在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止，就可以大大减少被网页恶意代码感染的几率。为了个人的网络安全，用户可以关闭 IE 中对 ActiveX 控件的支持，具体操作步骤如下：

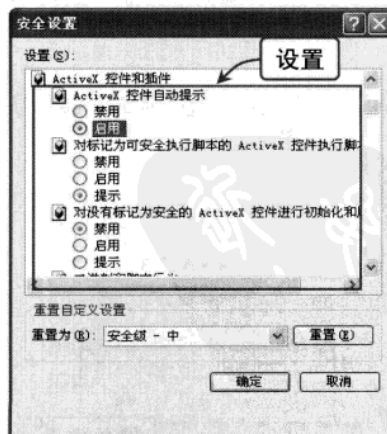
STEP 01 选择“安全”选项卡

运行 IE 浏览器，单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框。选择“安全”选项卡，单击“该区域的安全级别”选项区中的“自定义级别...”按钮，如下图所示。



STEP 02 ActiveX 控件设置

弹出“安全设置”对话框，可以对 ActiveX 控件进行详细设置，单击“确定”按钮，如下图所示。



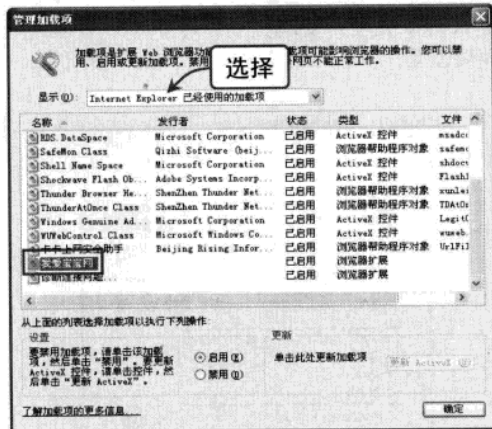
还可对 IE 浏览器中已经启用的 ActiveX 控件进行如下操作进行关闭：

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 09 网页恶意代码攻防

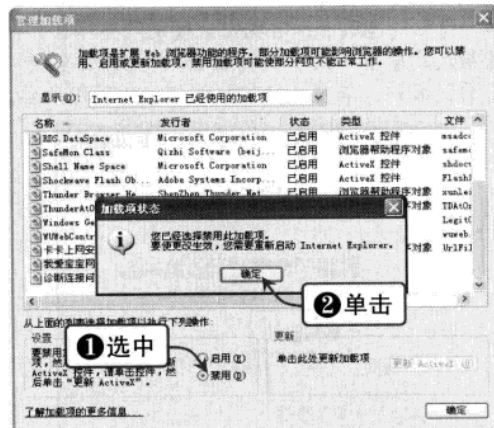
STEP 01 打开“管理加载项”

运行 IE 浏览器，单击“工具”|“管理加载项”命令，打开“管理加载项”对话框。在“显示”下拉列表框中选择“Internet Explorer 已经使用的加载项”选项，列表中显示当前 IE 浏览器中已经启用的 ActiveX 控件，如下图所示。



STEP 02 禁用 ActiveX 控件

在列表中选择已经开启的恶意的 ActiveX 控件，选中“设置”选项区中的“禁用”单选按钮，弹出“加载项状态”提示信息框，单击“确定”按钮，如下图所示。

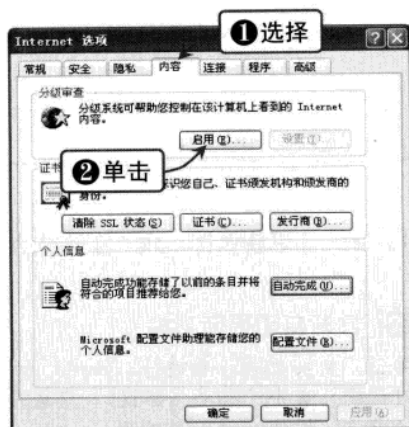


Work3 限制他人访问不良站点

在 IE 浏览器中可以对不良网站的访问进行限制。现在网络上的信息五花八门，良莠不齐，怎样限制使用同一电脑的其他用户浏览一些不良网站呢？可以进行如下操作：

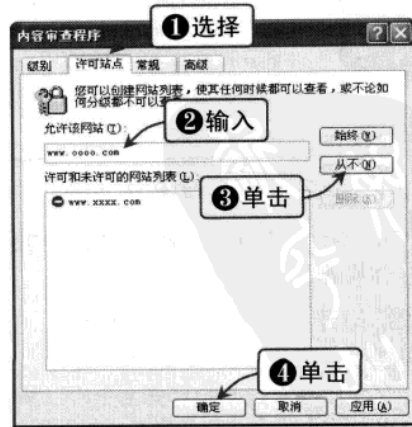
STEP 01 选择“内容”选项卡

运行 IE 浏览器，单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框，选择“内容”选项卡，单击“分级审查”选项区中的“启用”按钮，如下图所示。



STEP 02 设置限制站点

弹出“内容审查程序”对话框，选择“许可站点”选项卡。在“允许该网站”文本框中输入想要限制的网站地址，单击“从不”按钮，该网站就加入到下方网站列表中了，单击“确定”按钮，如下图所示。



基础入门
黑客入门
常用扫描工具
与嗅探工具
系统漏洞攻防
安全策略
设置系统
系统与文
件加密
远程控制
木马
聊天软件
网页恶意
代码攻防
电子邮件
C盘病毒
使用电脑
安全软件
黑客攻防
实用技巧

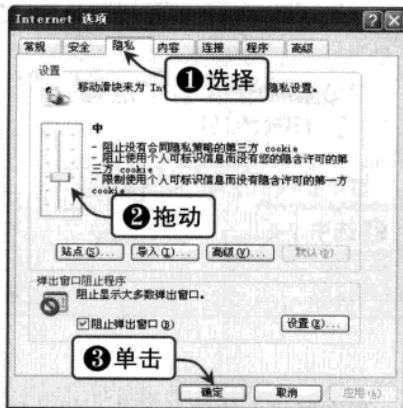


Work4 设置安全级别和隐私设置

设置安全级别和隐私设置是给一些高级用户使用的，一般用户在不太了解的情况下，使用默认设置即可，具体操作步骤如下：

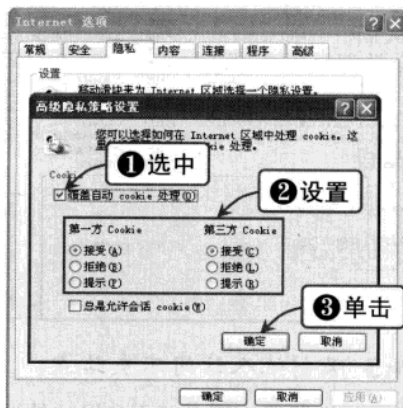
STEP 01 设置安全级别

运行 IE 浏览器，单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框，选择“隐私”选项卡，出现安全级别调整界面，拖动滑块或单击“默认”设置 IE 浏览器安全级别为默认级别，单击“确定”按钮，如下图所示。



STEP 02 隐私设置

单击“设置”选项区中的“高级”按钮，弹出“高级隐私策略设置”对话框，选中“覆盖自动 cookie 处理”复选框，并对 cookie 处理进行详细设置，单击“确定”按钮，如下图所示。



9.4.2 更新系统漏洞补丁

漏洞修复主要是指修复系统漏洞，一般应用程序的漏洞，主要是通过升级软件的版本来解决。作为 Windows 系统的开发商，微软也会不定期地发布一些系统漏洞补丁。用户可以使用下面介绍的几种方法进行更新。



提示

系统漏洞一般是由于系统服务对外部访问内部的验证机制有缺陷，导致某些别有用心的特殊代码通过时验证系统会发生崩溃，导致系统或者软件崩溃、用户权限提升、系统被控制等安全隐患。

IE 漏洞常见的有：浏览时自动运行恶意代码、后台自动下载文件并运行、蓝屏死机等。

Work1 打开系统自动更新功能

Windows 系统自身带有自动更新功能，可以与微软官方的更新保持一致，打开自动更新功能具体操作步骤如下：

STEP 01 打开“Windows 安全中心”

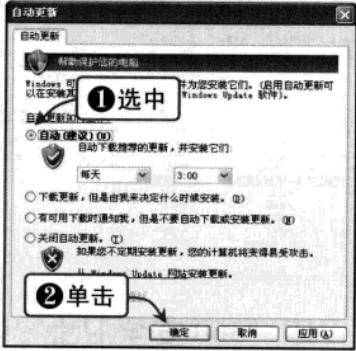
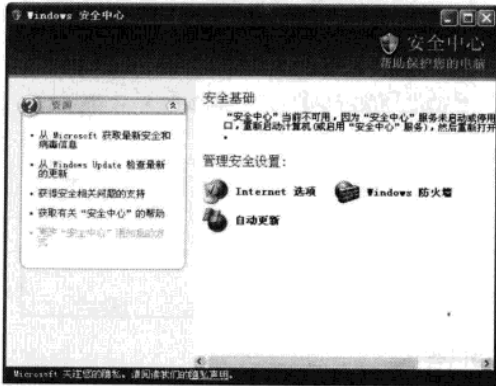
单击“开始”|“控制面板”命令，弹出“控制面板”窗口。单击“安全中心”按钮，显示“Windows 安全中心”窗口，如下图所示。

STEP 02 打开自动更新功能

单击“自动更新”超链接，弹出“自动更新”对话框。选中“自动（建议）”单选按钮。单击“确定”按钮，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 09 网页恶意代码攻防

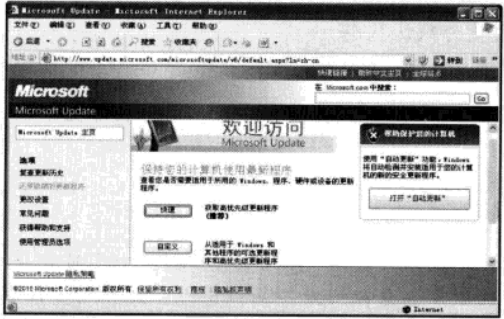


Work2 使用 IE 浏览器在线更新

用户可以使用 IE 浏览器自带的在线更新功能为电脑系统进行在线更新，具体操作步骤如下：

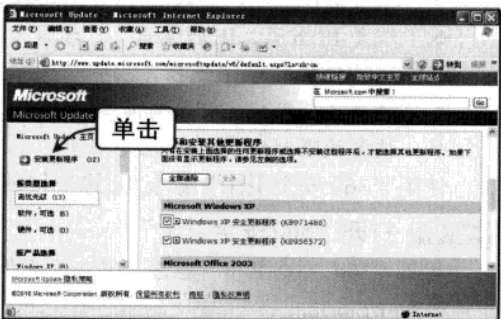
STEP 01 打开 Windows Update 页面

运行 IE 浏览器，单击“工具”| Windows Update 命令，IE 浏览器就自动连接到微软官方主页进行系统更新，如下图所示。



STEP 02 系统更新

单击“快速”按钮或“自定义”按钮，电脑会自动检测当前系统需要进行的更新，并把结果以列表方式显示。用户可以选中相应更新补丁对应的复选框，单击左侧的“安装更新程序”按钮，系统即可更新至最新状态，如下图所示。



Work3 使用第三方软件更新

使用第三方软件可以更加方便地对系统进行更新，下面将以使用“360 安全卫士”的“修复漏洞”功能为例介绍具体使用方法。

STEP 01 选择“修复漏洞”选项卡

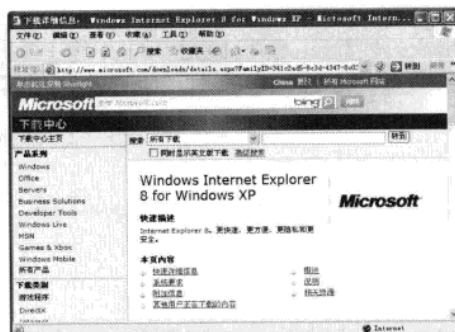
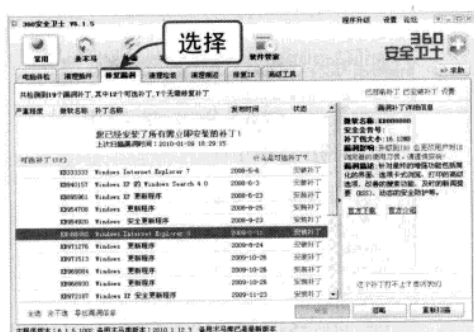
运行“360 安全卫士”软件，在主界面中选择“修复漏洞”选项卡，软件会自动对当前电脑系统进行扫描，并把需要进行的更新以列表的方式显示出来，如下图所示。

STEP 02 官方下载

选中要进行的更新，单击右窗格中的“官方下载”超链接，系统会自动调用 IE 浏览器打开官方地址进行下载，如下图所示。

- 基础入门
- 黑客入门
- 常用扫描
- 与嗅探工具
- 系统漏洞攻防
- Windows 系统
- 设置系统
- 安全策略
- 系统安全
- 文件加密
- 远程控制
- 木马攻防
- 聊天软件
- 网页恶意代码
- 电子邮件
- 病毒攻防
- 使用电脑
- 黑客攻防
- 应用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



9.4.3 用“360 安全卫士”修复 IE 浏览器

“360 安全卫士”是一款由奇虎网推出的功能强、效果好、很受用户欢迎的上网必备安全软件。“360 安全卫士”拥有木马查杀、恶意软件清理、漏洞补丁修复、电脑全面体检等多种功能。“360 安全卫士”的官方网站地址为 <http://www.360.cn>。

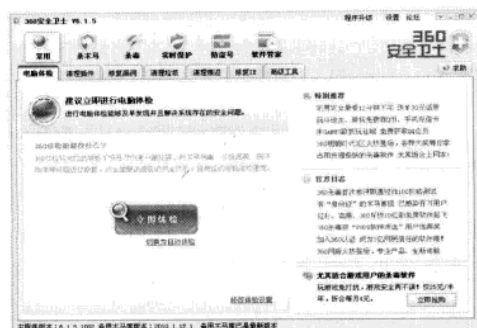
使用“360 安全卫士”可以对 IE 浏览器进行修复，其“IE 修复”功能有以下设置：

- ❖ 强力清除危险的进程项。
- ❖ 强力清除危险的 Windows 自启动项。
- ❖ 强力清除危险的 IE 右键快捷菜单额外项，IE 高级选项额外项和 IE 工具栏额外项。
- ❖ 强力清除危险的 IE 第三方工具条、BHO 插件、ActiveX 对象。
- ❖ 强力清除非法的计划任务。
- ❖ 恢复 hosts 文件为默认状态。
- ❖ 恢复协议关联、协议图标、文件关联为默认状态。
- ❖ 恢复 IE 首页、IE 搜索页、代理服务器设置为默认状态。
- ❖ 恢复被禁用的 IE 选项。
- ❖ 恢复被禁用的注册表编辑器。
- ❖ 恢复被限制的系统功能。

使用“360 安全卫士”修复 IE 浏览器的具体操作步骤如下：

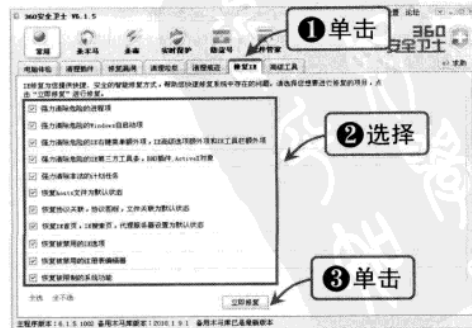
STEP 01 打开“360 安全卫士”

运行“360 安全卫士”程序，其主界面如下图所示所示。



STEP 02 修复 IE 浏览器

单击“常用”选项下的“修复 IE”选项卡，选中要修复内容对应的复选框，单击“立即修复”按钮，对 IE 浏览器进行修复，如下图所示。



Chapter 09 网页恶意代码攻防

9.4.4 使用“瑞星卡卡上网助手”

“瑞星卡卡上网助手”是一款基于互联网设计的全新反木马软件，可以有效拦截、防御、查杀各种木马病毒，并能帮助用户自动扫描并修补系统和第三方软件漏洞，优化电脑系统，是广大网民喜爱的安全软件，其具有以下功能：

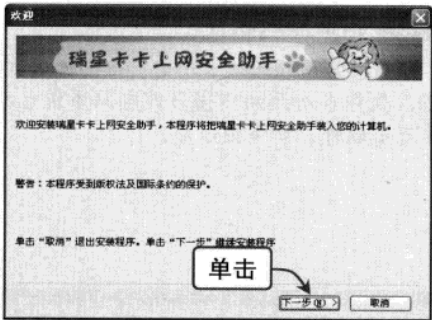
- ❖ 自动在线诊断，自动检测并提取电脑中的可疑样本。
- ❖ 依靠瑞星强大的反流氓软件技术，彻底清除系统中的流氓软件。
- ❖ 阻止U盘上的病毒运行，使其无法感染电脑。
- ❖ 自动修复操作系统漏洞、第三方软件漏洞和相关安全设置。
- ❖ 强力系统修复，使被病毒破坏的系统设置恢复正常。

Work1 安装“瑞星卡卡上网助手”

“瑞星卡卡上网助手”官方网站地址为 <http://tool.ikaka.com>，首先要下载并进行安装。

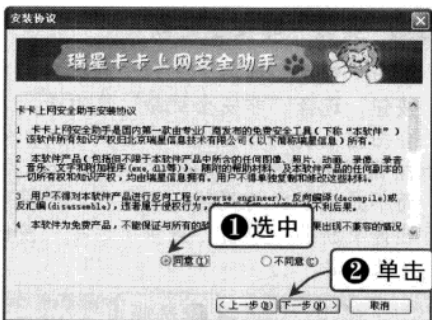
STEP 01 开始安装

运行安装文件，显示安装欢迎界面，单击“下一步”按钮，如下图所示。



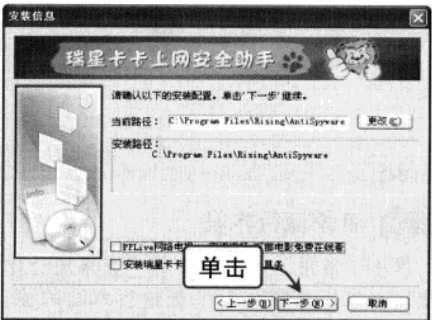
STEP 02 安装协议

在安装过程中弹出“安装协议”对话框，选中“同意”单选按钮，单击“下一步”按钮，如下图所示。



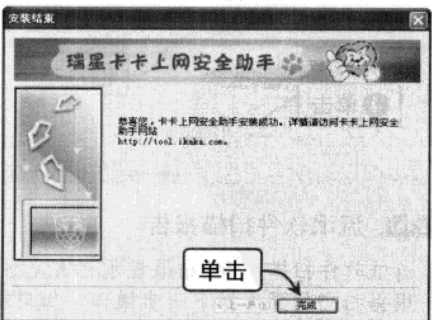
STEP 03 安装信息

在“安装信息”对话框中选择软件安装路径，单击“下一步”按钮，如下图所示。



STEP 04 完成安装

单击“完成”按钮，即可完成软件安装，如下图所示。



Work2 常用功能

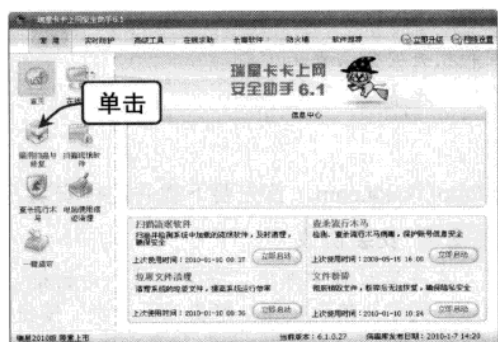
“瑞星卡卡上网助手”是一款综合安全软件，下面将具体介绍它的常用功能。

黑客
常用扫描
系统漏洞攻防
设置系统
安全策略
系统加密
远程控制
木马
聊天软
网页恶意
电子邮
C盘病
使用电脑
黑客攻防



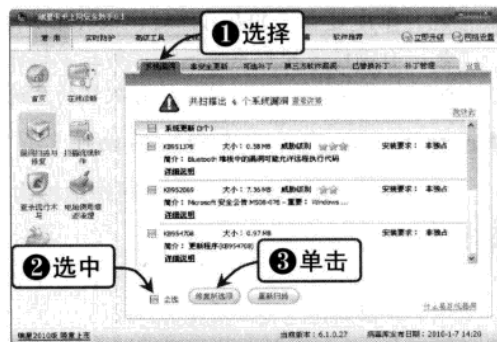
STEP 01 运行瑞星卡卡上网助手

单击桌面上的瑞星卡卡上网助手程序图标，启动瑞星卡卡上网助手，如下图所示。然后单击“常用”选项卡中的“漏洞扫描与修复”按钮。



STEP 02 修复系统漏洞

选择“系统漏洞”选项卡。瑞星卡卡上网助手会对照微软官方发布的系统漏洞，检查当前电脑系统，并把结果以列表形式显示。如下图所示，扫描出4个系统漏洞。选中“全选”复选框，单击“修复所选项”按钮，进行系统漏洞的修复工作。



STEP 03 安装“非安全更新”

单击“常用”选项卡中的“漏洞扫描与修复”按钮，选择“非安全更新”选项卡。上网助手会扫描系统所需要的非安全更新。非安全更新指微软针对操作系统发布的功能上的更新，而不是安全类的更新，用户可以根据需要进行选择更新项，单击“更新所选项”按钮，如下图所示。



STEP 04 扫描流氓软件

单击“常用”选项卡中的“扫描流氓软件”按钮，软件自动开始扫描当前电脑系统已经安装的流氓软件，如下图所示。



STEP 05 流氓软件扫描报告

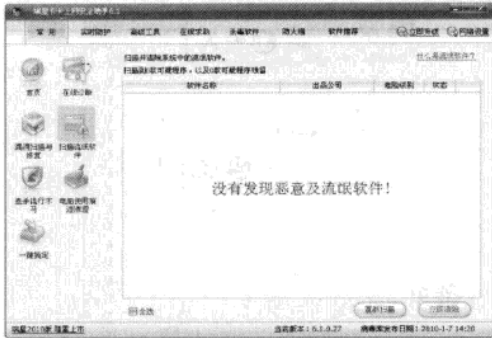
流氓软件扫描完毕，结果显示在右窗格中。用户根据扫描结果选择下一步操作，如果有流氓软件，则可以单击“立即清除”按钮，如下图所示。

STEP 06 查杀流行木马

单击“常用”选项卡中的“查杀流行木马”按钮，可以对当前电脑系统进行木马的检查和清除。在“扫描对象”选项区中选择目标，单击“开始扫描”按钮，如下图所示。


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 09 网页恶意代码攻防



STEP 07 清理电脑使用痕迹

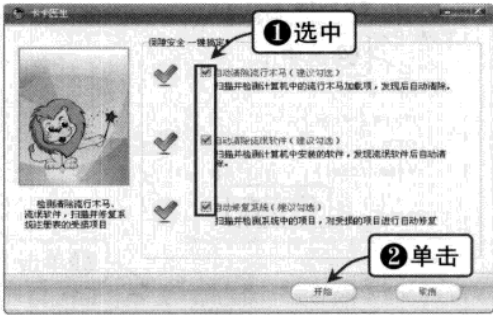
使用“电脑使用痕迹清理”功能可以防止他人查看自己的使用记录，有效地保护电脑用户的隐私。单击“常用”选项卡中的“电脑使用痕迹清理”按钮，在右窗格中选择要清理的具体项目，设置完成后单击“清理”按钮，开始清理使用痕迹，如下图所示。






STEP 08 使用“一键搞定”功能

单击“常用”选项卡中的“一键搞定”按钮，弹出“卡卡医生”窗口，选中“自动清除流行木马”、“自动清除流氓软件”和“自动修复系统”三个复选框，单击“开始”按钮，如下图所示。





提示

对于一般的电脑用户来讲，在电脑出现问题后，直接使用“一键搞定”功能不失为一种非常省时、省力的方法。

Work3 实时防护

“瑞星卡卡上网助手”还具有“实时防护”功能，具体使用方法如下：

STEP 01 实时防护

在软件主界面中单击“实时防护”选项卡中的“本机防护”按钮，此时右窗格中显示“自动在线诊断”、“U 盘病毒免疫”、“自动修复系统漏洞”和“不良网站访问防护”四项功能，用户可以根据需要单击“启用”或“禁用”按钮，如下图所示。

STEP 02 自动诊断求助设置

单击“自动在线诊断”选项区的“高级设置”超链接，弹出“自动诊断求助设置”窗口。在“请填写您的邮箱地址”文本框输入自己的邮箱地址，并设置自动在线诊断频率，单击“确定”按钮，如下图所示。

基础入门
黑客
常用扫描
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码防
击
电子邮箱
C盘病
使用电
脑安全
软件
黑客攻
防技巧

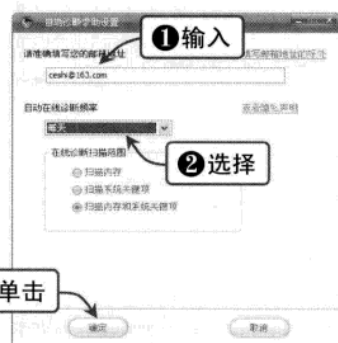
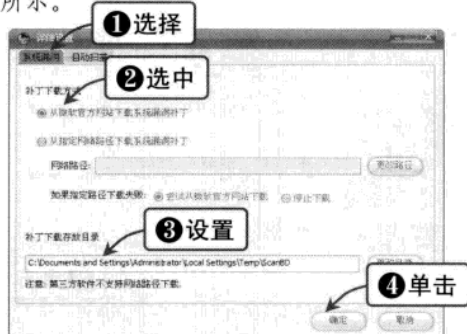
219

溜客安全网 WwW.176Ku.CoM



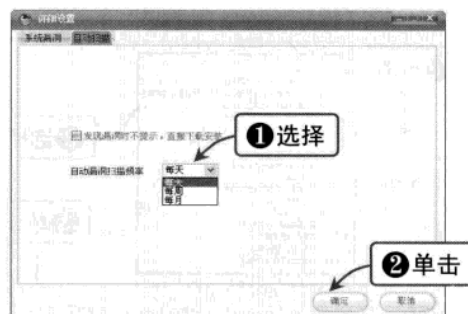
STEP 03 补丁下载设置

单击“自动修复系统漏洞”选项区的“高级设置”超链接，弹出“详细设置”窗口，选择“系统漏洞”选项卡。选中“从微软官方网站下载系统漏洞补丁”单选按钮，并设置补丁下载存放目录，然后单击“确定”按钮，如下图所示。



STEP 04 自动扫描漏洞设置

选择“自动扫描”选项卡，在“自动漏洞扫描频率”下拉列表框中选择“每天”选项，单击“确定”按钮，如下图所示。



提示

建议经常使用电脑的用户把“自动漏洞扫描频率”设置为“每天”，这样在每天开机时就会自动进行漏洞扫描，保证第一时间为电脑进行安全检查。

Work4 高级工具

下面将介绍“瑞星卡卡上网助手”的高级功能，具体操作步骤如下：

STEP 01 启动项管理

单击“高级工具”选项卡中的“启动项管理”按钮，程序会自动扫描当前系统的启动项目，结果以列表形式显示在右窗格中。选择要操作的启动项目并右击，在弹出的快捷菜单中选择“禁用”选项，如下图所示。

STEP 02 进程管理

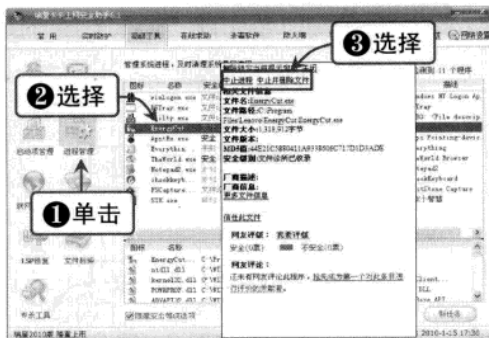
单击“高级工具”选项卡中的“进程管理”按钮，程序会自动扫描系统当前的实时进程，结果以列表形式显示在右窗格中。单击要操作的进程，弹出提示信息框，显示该进程的详细信息，根据需要单击“中止进程”或“中止并删除文件”超链接，如下图所示。

Chapter 09 网页恶意代码攻防



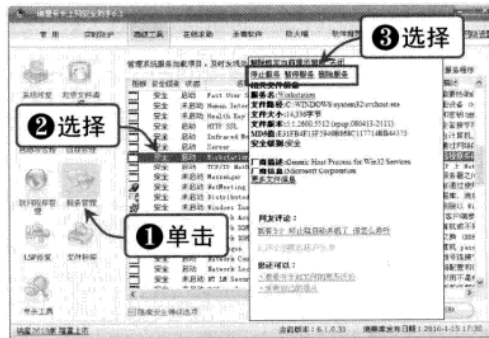
STEP 03 联网程序管理

单击“高级工具”选项卡中的“联网程序管理”按钮，程序会自动扫描系统当前的实时连接网络的程序，结果以列表形式显示在右窗格中。单击要操作的程序，弹出提示信息框，显示该程序的详细信息，根据需要单击“结束进程”或“关闭连接”超链接，如下图所示。



STEP 04 服务管理

单击“高级工具”选项卡中的“服务管理”按钮，程序会自动扫描系统当前开启的系统服务，结果以列表形式显示在右窗格中。单击要操作的服务，弹出提示信息框，显示该服务的详细信息，根据需要单击“停止服务”、“暂停服务”或“删除服务”超链接，如下图所示。



提示



Windows 系统在启动时会默认启动一些系统服务，而这些启动服务不一定是每个用户都需要的，用户可以根据自己个人的情况来关闭和停止一些不需要的服务，这样能够更加节省系统资源，提高系统的工作效率。

STEP 05 文件粉碎

使用文件粉碎功能可以更加有效地防止已经删除的文件被有目的地恢复。单击“高级工具”选项卡中的“文件粉碎”按钮，在右窗格中选择要删除的文件名或目录名，单击“粉碎”按钮，弹出“提示”信息框，单击“是”按钮，完成文件的粉碎，如下图所示。

STEP 06 专杀工具

瑞星提供了一系列的病毒专杀工具，用户可以通过“瑞星卡卡上网助手”的“专杀工具”进行调用。单击“高级工具”选项卡中的“专杀工具”按钮，右窗格中显示专杀工具列表，单击要使用的专杀工具超链接，程序会自动调用 IE 浏览器打开该专杀工具的下载网页，用户可以自行下载使用，如下图所示。

基础知识

与嗅探工具

系统漏洞攻防

安全策略

系统与安全

远程控制

木马攻防

代码攻防

件攻防

件攻防

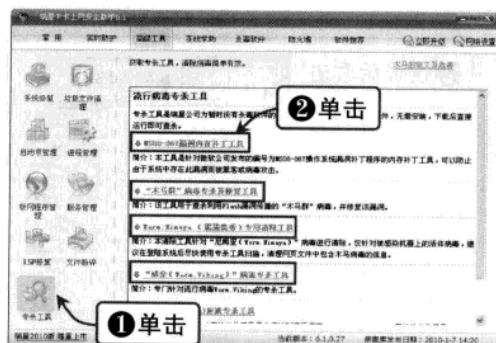
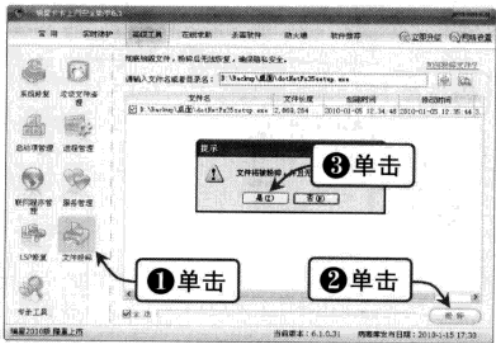
件攻防

件攻防

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

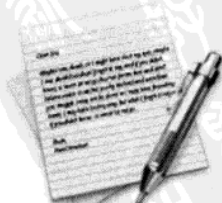


黑客攻防从新手到高手



● 读书笔记

Blank lined area for taking notes.



Chapter

10

电子邮件攻防

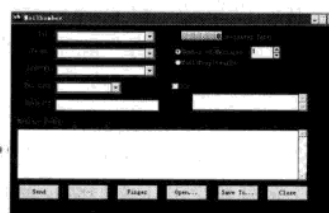
随着电脑与网络的快速普及，电子邮件作为便捷的传输工具，在信息交流中发挥着重要的作用。很多大中型企业和个人已实现了无纸办公，所有的信息都以电子邮件的形式传送着，其中包括很多商业信息、工业机密和个人隐私，因此，电子邮件的安全成为人们重点考虑的问题。本章将详细讲解电子邮件的攻击和防范技术。

本章建议学习时间：

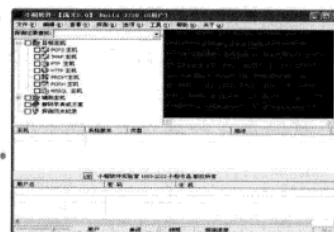
本章建议学习时间为 50 分钟，其中分配 30 分钟学习电子邮件攻防技术的相关知识，20 分钟观看教学视频课件并进行练习。

学完本章后您可以：

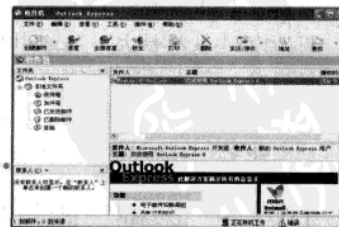
- 了解电子邮件病毒的特征
- 了解邮件炸弹的原理和危害
- 学会制造邮件炸弹
- 学会使用工具破解邮箱密码
- 学会防范邮件炸弹的攻击
- 学会防范邮件病毒的感染



设置 MailBomber 选项



运行流光程序



打开 Outlook Express



重要知识点视频索引



10.1 电子邮件病毒

电子邮件本身不会产生病毒，只是病毒的寄生场所。电子邮件病毒是指通过电子邮件传播的病毒，一般嵌入邮件的附件中，在用户运行附件中的病毒程序后，就会使电脑染毒。

10.1.1 “邮件病毒”定义及特征

“邮件病毒”其实和普通的电脑病毒一样，只不过由于它们的传播途径主要是通过电子邮件，所以才被称为“邮件病毒”。电子邮件病毒通常是把自己作为附件发送给被攻击者，如果接收到该邮件的用户不小心打开了附件，病毒即会感染用户的电脑。更可怕的是，带有尼姆达病毒的电子邮件，不需要打开附件，只要阅读或预览了带病毒的邮件，那么电脑就很可能受到病毒的侵害，并且还会沦为病毒的帮凶，继续发送带病毒的邮件给通讯簿中的朋友。现在大多数电子邮件病毒都会在感染用户的电脑之后自动打开 Outlook 中的地址簿，然后把病毒自身发送给地址簿上的每一个电子邮箱中，这正是电子邮件病毒能够一下子大面积传播的原因所在。另外，电子邮件客户端程序的一些 Bug 也可能被攻击者利用来传播电子邮件病毒。微软的 Outlook 曾经有两个漏洞被攻击者所利用，使邮件附件中的病毒程序可以不用打开即可自动运行。

“邮件病毒”除了具备普通病毒可传播性、可执行性、破坏性、可触发性特征之外，还具有以下几个特征：

- ❖ 感染速度快：在单机环境下，病毒只能通过 U 盘或光盘等介质，从一台电脑传染到另一台。而在互联网中，绝大多数通过电子邮件传播的病毒都有自我复制和传播的能力，这正是它们的危险之处。它们不仅能够用户在发送邮件时把病毒自身进行复制传播，而且还能够主动选择用户邮箱地址簿中的地址并发送带有病毒的邮件。根据测定，网络在正常使用的情况下，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台电脑全部感染。

- ❖ 扩散面广：由于企业邮箱的邮件不仅仅在单个企业内部传播，还在互联网内传送，这直接导致邮件病毒的扩散不仅快，而且扩散范围很大，不但能迅速传染局域网内所有电脑，还能将病毒在一瞬间传播到千里之外。当其发作时，甚至可以造成整个网络的瘫痪，因此造成的损失往往是难以估计的。

- ❖ 清除病毒困难：单机上的电脑病毒有时可通过删除带毒文件、格式化硬盘等措施将病毒彻底清除。而企业中的电脑一旦感染了病毒，清除病毒会变得非常困难，刚刚完成清除工作的电脑就有可能被网络中另一台带毒工作站所感染，使得清除邮件病毒变得非常困难。

- ❖ 破坏性大：网络中的电脑感染了邮件病毒之后，将直接影响网络的工作效率，轻则降低速度，影响工作效率，重则使网络及电脑崩溃，资料丢失。

- ❖ 隐蔽性：邮件病毒与其他病毒相比，更加隐蔽。一般来说，邮件病毒通常是隐藏在邮件的附件中，或是邮件的信纸模板中，这在一定程度上会加速病毒的泛滥，也增加了查杀病毒的难度。

10.1.2 识别“邮件病毒”

要想防范“邮件病毒”，必须能够准确地对其进行识别。下面将介绍三个识别“邮件病

毒”的技巧：

- ❖ 查看附件大小。电子邮件的附件通常是“邮件病毒”的最佳载体，通常查看附件大小，就可以识别电子邮件是否携带病毒。如果发现电子邮件的附件大小异常，则该邮件则有可能携带病毒。
- ❖ 查看邮件地址。“邮件病毒”的传播者通常利用一些陌生的邮件地址发送邮件，当收到来自陌生地址的邮件时，一定加倍小心。如果这类邮件有附件，更要谨慎，因为其极有可能携带病毒。对于陌生邮件，在看了邮件地址后，再看邮件内容无关痛痒且与工作无关，基本可以判定该邮件携带病毒。
- ❖ 识别真伪退信。用户书写邮件时，如果将收件人的邮件地址写错，邮件服务器会自动将该邮件退回。一些“邮件病毒”利用退信中的附件，该附件书写着用户邮件正文。一旦用户打开假冒的邮件服务器退信，并且查看了附件，“邮件病毒”将会立刻感染用户的电脑。

10.2 认识电子邮件炸弹

电子邮件炸弹是最常见的匿名攻击之一，通过设置一台机器不断大量地向同一地址发送电子邮件，攻击者能够耗尽接受者网络的带宽。由于这种攻击方式简单易用，也有很多发匿名邮件的工具，而且只要获悉被攻击者的电子邮件地址就可以进行攻击，所以这是大家最值得防范的一个攻击手段。

10.2.1 电子邮件炸弹的定义和危害

电子邮件炸弹也称为 E-mail Bomber，是黑客常用的攻击手段之一。具体指的是电子邮件的发送者利用某些特殊的电子邮件软件，在很短时间内连续不断地将大容量的电子邮件邮寄给同一个收信人，而一般收信人的邮箱容量是有限的，在这些数以千计的大容量信件面前肯定是不堪重负，而最终“爆炸身亡”。这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至还能影响到邮件系统所在的服务器系统的安全。

电子邮件炸弹的危害在于它可以大量消耗网络资源，常常导致网络塞车，使大量的用户不能正常工作。通常，因特网服务商给一般的网络用户的信箱容量都是有限的，而在这有限的空间中除了处理电子邮件之外，还得用它来存储一些下载下来的软件，或者是存储一些自己喜欢的网页内容。如果用户在短时间内收到成千上万封电子邮件，而每个电子邮件的容量也比较大，那么经过一轮邮件炸弹轰炸后很容易就把用户有限的容量挤垮。如果是这样的话，用户的电子邮箱中将没有任何多余的空间接纳其他的邮件，那么其他人寄给用户的电子邮件将会丢失或者被退回，这时用户的邮箱已经失去了作用。

另一方面，这些电子邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞带宽并不富裕的传输信道；而且用户的网络接入服务提供者需要不停地忙着处理大量的电子邮件的来往，这样会加重服务器的工作强度，减缓了处理其他用户的电子邮件的速度，从而导致了整个网络的延迟。

如果网络接入服务提供者承受不了这样的疲劳工作，网络随时都会瘫痪，严重的可能会引发整个网络系统崩溃。

黑客

常用扫描与嗅探工具

Windows系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制攻防

木马攻防

聊天软件攻防

网页恶意代码攻防

电子邮件攻防

C语言病毒攻防

使用电脑安全软件

黑客攻防实用技巧

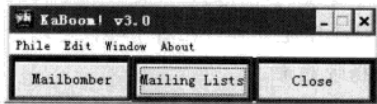


10.2.2 电子邮件炸弹的制作

KaBoom 是一款经典的邮件炸弹程序，它可以不间断地进行发信，而且内置了常用的匿名邮件服务器地址。下面将以 KaBoom 3.0 为例，介绍其基本用法。

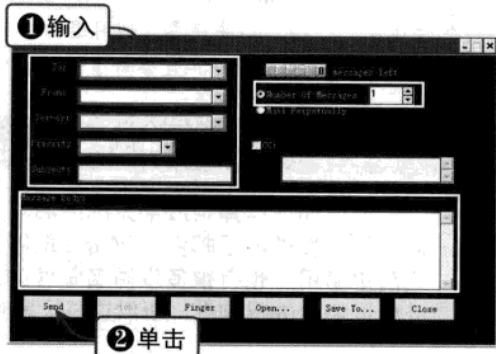
STEP 01 打开 KaBoom 程序

启动 KaBoom 3.0 后会显示程序主窗口，上面有三个按钮：MailBomber（炸弹）、Mailing Lists（为别人订邮件组）和 Close（退出），如右图所示。



STEP 02 设置 MailBomber 选项

单击主窗口中的 MailBomber 按钮，打开 MailBomber 窗口。在 To 文本框中输入收件人的地址，在 From 文本框中输入姓名或冒充别人的名字，在 Server 下拉列表框中选择一个匿名邮件服务器，在 Subject 文本框中输入信件标题，在 Message Body 文本框中输入信件内容，在 Number of Messages 数值框中输入炸弹数量，单击 Send 按钮开始发送，如右图所示。



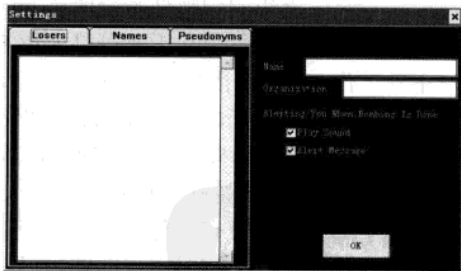
STEP 03 设置 Mailing Lists 选项

单击主窗口中的 Mailing Lists 按钮，打开 Mailing Lists 窗口。在左窗格中选择要订阅的邮件组，在 Address 文本框中输入收件人，在 Server 下拉列表框中选择一个匿名邮件服务器，单击 Subscribe 按钮确定要选择的邮件组，如下图所示。



STEP 04 程序设置

单击 Edit | Settings 命令，弹出 Settings 对话框。Losers 显示被攻击目标列表，Names 显示常用的匿名，Pseudonyms 显示常用的假地址。Play Sound 复选框是音效开关，Alert Msg 复选框是详细报告开关。单击 OK 按钮完成设置，如下图所示。



10.3 常见获取电子邮件密码手段

黑客对于电子邮件的攻击，除了大量放置“邮件炸弹”外，还经常利用一些黑客软件来探测邮箱地址，并使用暴力破解程序进行密码破解，从而达到获取邮件中的重要信息，或向地址簿中的邮箱地址发送病毒的目的。下面将介绍几种用来破解邮箱密码软件的使用方法。

Chapter 10 电子邮件攻防

10.3.1 使用流光

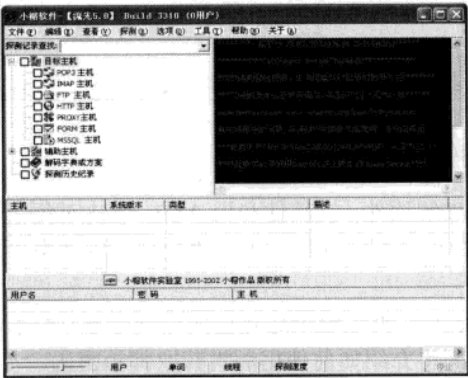
“流光”是一款绝好的 FTP、POP3 解密工具，在破解密码方面，它具有以下功能：

- ❖ 加入了本地模式，在本机运行时不必安装 Sensor。
- ❖ 用于检测 POP3/FTP 主机中用户密码安全漏洞。
- ❖ 高效服务器流模式，可同时对多台 POP3/FTP 主机进行检测。
- ❖ 支持 10 个字典同时检测，提高破解效率。

使用“流光”破解密码的具体操作步骤如下：

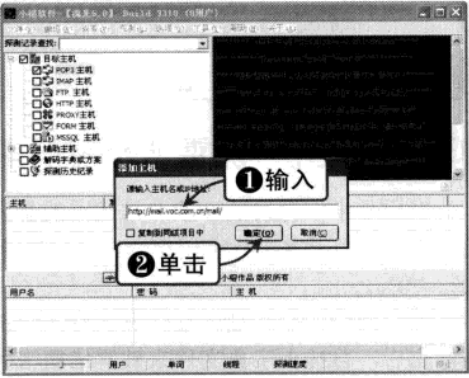
STEP 01 运行流光程序

运行“流光”程序，主窗口如下图所示。选中“POP3 主机”复选框，单击“编辑”|“添加”|“添加主机”命令。



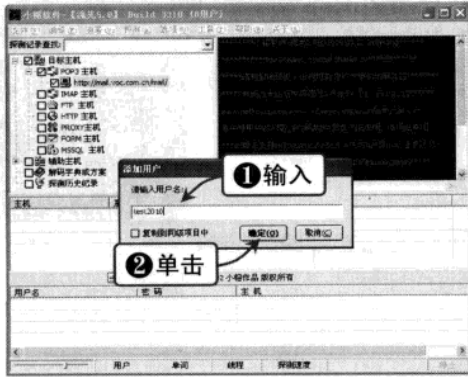
STEP 02 确定目标

弹出“添加主机”对话框，在文本框中输入要破解的 POP3 服务器地址，单击“确定”按钮，如下图所示。



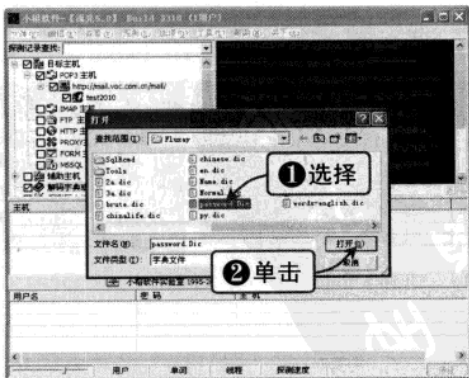
STEP 03 确定用户名

选中刚添加的服务器地址前的复选框，然后单击“编辑”|“添加”|“添加用户”命令，弹出“添加用户”对话框，在文本框中输入要破解的用户名，单击“确定”按钮，如下图所示。



STEP 04 选择字典文件

选中“解码字典或方案”复选框，单击“编辑”|“添加”|“添加字典”命令，弹出“打开”对话框，选择要添加的字典文件，单击“打开”按钮，如下图所示。

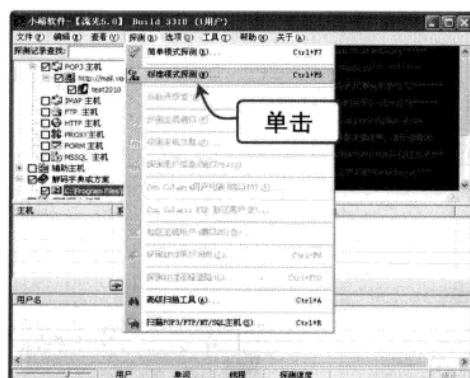


黑客
基础知识
常用扫描
与嗅探工具
漏洞攻防
系统与安全
设置策略
安全策略
系统与安全
件加密
远程攻击
制攻击
攻防
木马
聊天软
件攻击
网页恶
意代码
攻防
电子邮
件攻击
C 盘病
毒攻防
使用电脑
安全软件
黑客攻
防技巧



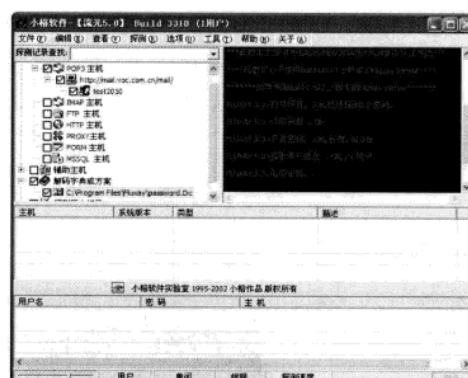
STEP 05 选择探测模式

单击“探测”|“标准模式探测”命令（“简单模式探测”功能不用指定具体的字典文件，使用流光内置的简单密码），如下图所示。



STEP 06 开始探测

流光开始进行探测，右窗格中显示实时探测过程。如果字典选择正确，就会破解出正确的密码，如下图所示。



10.3.2 使用“溯雪 Web 密码探测器”

溯雪是小榕开发的一款非常优秀的暴力密码破解软件，该软件利用 ASP、CGI 对免费信箱、论坛、聊天室进行密码探测。密码探测主要是通过穷举数字的方法来实现，成功率可达 60%~70%。

溯雪的运行原理是通过提取 ASP、CGI 页面表单，搜寻表单运行后的错误标志，有了错误标志后，再挂上字典文件来破解信箱密码。下面将介绍如何使用溯雪获取邮箱密码。

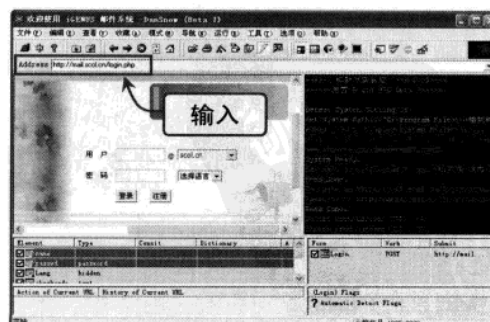
STEP 01 运行溯雪程序

运行“溯雪”程序，主窗口显示如下图所示。



STEP 02 确定目标

在“Address（地址）”文本框输入要登录邮箱的地址，按【Enter】键。溯雪会跳转到该地址所对应的页面，单击“文件”|“从当前 URL 导入”命令，在 Element（元素）区域中会出现页面表单的内容，如下图所示。

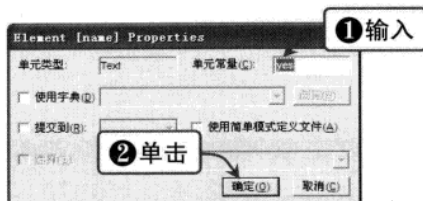


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 10 电子邮件攻防

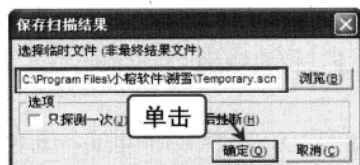
STEP 03 确定用户名

双击表单中的 name 项，将会弹出 Element [name]Properties 对话框，在“单元常量”文本框中输入 yes（此处以破解用户名为 yes 的邮箱密码为例），单击“确定”按钮，如下图所示。



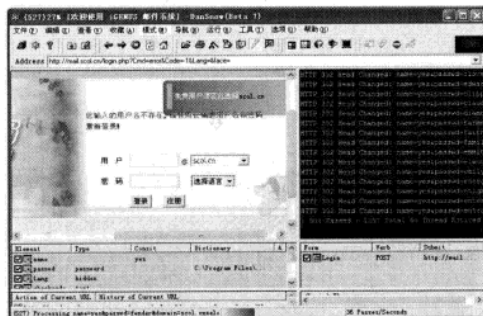
STEP 05 设定结果保存位置

单击“运行”|“开始/重新开始”命令，弹出“保存扫描结果”对话框。使用默认位置，单击“确定”按钮，如下图所示。



STEP 07 开始探测

溯雪开始探测，并在右窗格中显示实时探测过程，如下图所示。



10.3.3 使用“黑雨”软件暴力破解

黑雨是一款通过流行的 POP3 协议进行邮箱账号密码破解的黑客工具软件。黑雨利用“穷举法”进行远程暴力破解密码，它可以支持字符方式、自定义字符、字典方式、字串方式四

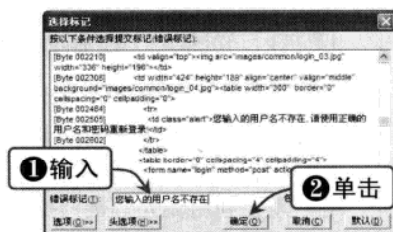
STEP 04 选择字典文件

双击表单中的 `passwd` 项, 将会弹出 `Element [passwd]Properties` 对话框, 选中“使用字典”复选框, 并单击“浏览”按钮, 选择具体要使用的字典文件 (溯雪自带了一些破解词典, 如果这些字典不能满足要求, 可以用字典生成工具生成个人字典), 如下图所示。



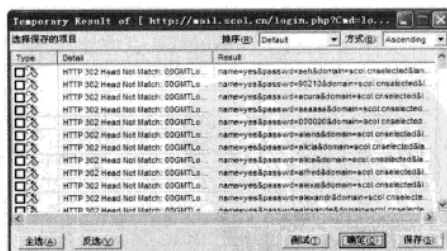
STEP 06 设置错误标志

溯雪进行一次探测，弹出“选择标记”对话框，将提示的错误信息“您输入的用户名不存在”输入到“错误标记”文本框中，单击“确定”按钮，如下图所示。



STEP 08 探测结束

溯雪探测结束，将会出现一个结果报告单。如果字典选择正确，就会破解出正确的密码，如下图所示。





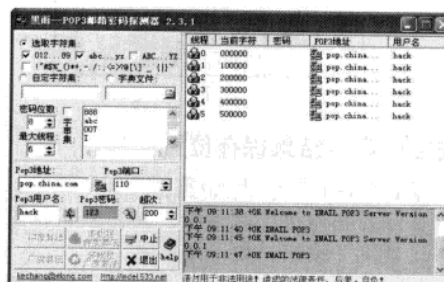
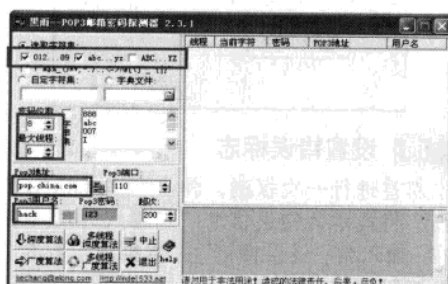
种不同的方式进行密码计算，使用方法如下：

STEP 01 打开程序

运行黑雨软件，在主窗口中选择数字、小写字母、大写字母或字符复选框，设定密码的组成范围。“密码位数”设为8位，“最大线程”设为6。以破解服务器 pop.china.com 上的 hack 用户的邮箱密码为例，在“Pop3 地址”文本框中输入 pop.china.com，在“Pop3 用户名”文本框中输入 hack，如下图所示。

STEP 02 开始破解

单击“多线程广度算法”按钮，程序开始对选中的邮箱用户进行密码穷举破解。实时过程显示在右窗格中。单击“中止”按钮，停止破解，单击“退出”按钮，即可退出程序，如下图所示。



10.3.4 使用“流影”破解邮箱密码

流影是一个和流光功能相似的工具，和流光最大的不同在于，流影是运行于用户主机也就是客户端的，是一个图形界面的工具，而流影可以同时运行于服务器端和客户端，用户可以通过 telnet 来进行远程管理和控制。

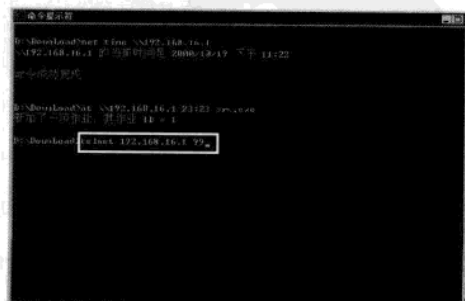
首先，用户需要利用流光等端口探测软件，查找到一个有开放端口的电脑，如本例中使用 IP 地址为 192.168.16.1 的电脑，其开放端口为 137，用户名为 administrator，口令为 123456，需要破解密码的邮箱地址为 fybugang12@21cn.com。

STEP 01 复制文件

登录远程主机后，利用 DOS 下的 copy 命令复制 fspop.exe、srv.exe 以及 user.sch 文件到目标机器，其中 fspop.exe 和 srv.exe 在流影的安装文件夹中能够找到，user.sch 是方案文件，如下图所示。

STEP 02 启动 srv 进程，并启动服务

复制完成以后，用 at \192.168.16.1 23:23 srv.exe 命令启动 srv 进程，然后使用 telnet 命令进行登录，如下图所示。

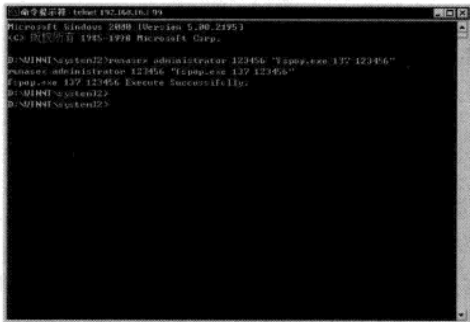


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 10 电子邮件攻防

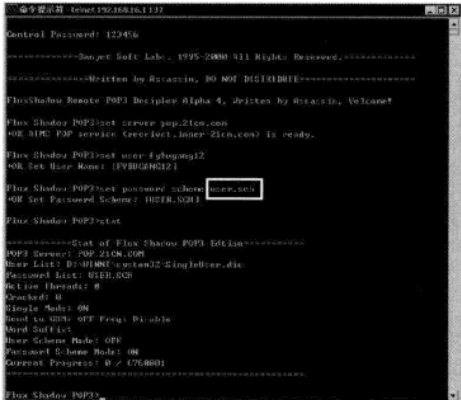
STEP 03 创建 Fspop.exe 进程

输入 RunasEx 命令：runasex administrator 123456 "fspop.exe 137 123456"，创建 Fspop.exe 进程，其中 administrator 是管理员用户名，123456 是登录口令，如下图所示。



STEP 04 开始破解

首先登录到已经扫描到的开放端口，本例中的开放端口为 137，开始破解账号为 fybugang12@21cn.com 的密码，采用的破解方案的文件名为 user.sch，如下图所示。



10.4 防范电子邮件攻击

电子邮箱是重要的网络交流工具，具有方便、快捷、实时的特点。在电子邮箱中，我们也经常存放一些重要的信件和信息。一旦邮箱受到攻击，很可能泄露邮件中的重要信息，并可能导致网络瘫痪。因此，我们更应该重视保护邮箱安全。下面将详细介绍如何防范电子邮件攻击。

10.4.1 重要邮箱的保护措施

重要邮箱是用户用于存放比较重要的邮件和信息的邮箱，需要采取一些措施进行保护。我们知道，一般邮件攻击的前提是要知道用户的邮箱才可以进行下一步的攻击活动，因此，为了避免遭到攻击，我们应该尽量做到不轻易把自己的重要邮箱地址泄露给他人，并设置安全的密码等防范工作。

Work1 使用备用邮箱

建议用户不要轻易把自己的重要邮箱地址泄露给他人，但在某些网站或 BBS 上，需要用户进行邮箱注册才能实现浏览和发帖等功能；或是在工作中需要用邮箱进行交流、发布信息等，这时就需要我们使用备用邮箱了。

用户可以申请一个免费邮箱作为备用邮箱，可以利用这个邮箱订阅新闻、电子杂志，放在自己的个人主页上，在自己感兴趣的论坛或者 BBS 上使用，或是用于代表公司对外进行业务联系。

需要注意的是，如果是利用了备用邮箱进行过一些必要的网络服务申请，应该把确认信息再转发到自己的私人邮箱中备用。

- 黑客
- 常用扫描
- 系统漏洞攻防
- 设置系统
- 系统与安全
- 系统加密
- 远程控制
- 木马
- 聊天软件
- 网页恶意
- 代码攻防
- 电子邮件
- C盘病毒
- 使用电脑
- 黑客攻防



Work2 保护邮箱密码

除了要保护好重要邮箱的地址以外，邮箱的密码也是需要重点保护的。可以采取以下几种方式来防止攻击者进行暴力破解：

- ❖ 密码选择。密码至少要有 8 位，并且密码里要包括至少一个数字，一个大写字母和一个小写字母，最好能包括一个符号。这种字母、数字和符号组成的密码，对于暴力破解软件来说，是不易破解的。另外，密码最好不要包括用户的名字缩写、生日、手机号、公司电话等公开信息。

- ❖ 定期更改密码。要养成定期更改密码的习惯，最好每个月更改一次密码，这样会大大增加破解密码的难度。

- ❖ 启用邮箱密码保护功能。通过设置密码保护，可以在忘记密码时通过回答密码提示问题或发送短信验证的方式取回密码。

10.4.2 找回邮箱密码

如果用户不小心忘记邮箱密码后，可以登录提供邮箱的 POP3 服务器，现在一般的免费邮箱供应商都提供密码找回功能。比如，现在比较常用的 163 网易免费邮箱，它提供了“通过密码提示问题”、“通过保密邮箱”、“通过手机”、“通过安全码”等多种方式找回用户的邮箱密码。下面以“通过密码提示问题”为例，介绍找回密码的具体操作方法。

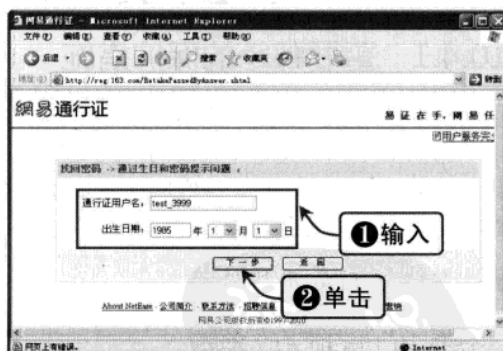
STEP 01 进入密码修复界面

在地址栏中输入 <http://reg.163.com/Recover-Passwd1.shtml?from=mail163>，进入密码修复界面。选择要找回密码的方式，在此使用“通过密码提示问题”方式。单击相应的超链接，如下图所示。



STEP 02 输入正确信息

在弹出的页面中输入要找回密码的用户名，并正确输入用户在注册邮箱时输入的出生日期，输入完毕后，单击“下一步”按钮，如下图所示。



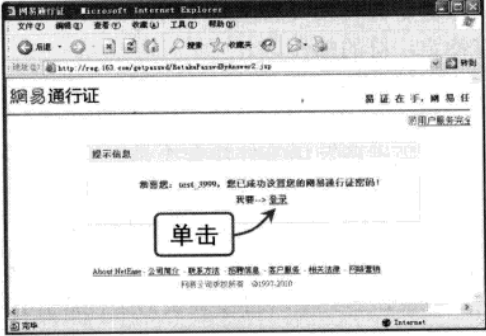

STEP 03 回答提示问题

在“找回密码”页面中正确填写密码提示问题的答案，并输入新密码和验证文字，单击“下一步”按钮，如下图所示。

STEP 04 重置密码成功

重置密码成功后会出现信息提示框，可以通过单击“登录”超链接直接登录邮箱，如下图所示。

Chapter 10 电子邮件攻防



10.4.3 防止炸弹攻击

攻击者一旦通过地址扫描或有目的地获取了用户的邮箱地址，就可以利用邮件炸弹工具对用户的邮箱进行炸弹攻击，直至网络瘫痪。因此，我们要提高对“邮件炸弹”的防范意识，从根本上解除“邮件炸弹”的威胁。

- 1. 邮件地址保密**

在进行上网活动时，尽量不要暴露自己的重要邮箱地址。如果需要通过邮箱注册定制网络服务时，请使用另外申请的备用邮箱。
- 2. 隐藏邮件地址**

攻击者通常利用工具进行邮件地址搜索，我们可以通过隐藏邮箱地址的方法躲过搜索。如将 test@163.com 在输入时改成 test.#163.com，这样一来大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。
- 3. 使用垃圾邮件拦截工具**

目前大多数电子邮件服务提供商都会利用一些智能技术来自动拦截大多数垃圾邮件，阻止垃圾邮件进入用户邮箱。用户可以发现，邮箱中经常会有邮件出现在“垃圾邮件”文件夹下，因为电子邮件服务提供商会对接收到的邮件进行智能筛选，将可疑的邮件都发送到了这里，而最后由用户自己来进行判断是否垃圾邮件。通过邮件服务商的过滤后，垃圾邮件的确会大幅减少。
- 4. 谨慎使用“自动回复”功能**

许多用户在邮件系统中设置使用了“自动回复”功能，当用户的邮箱系统发现新邮件而又不能及时回复时，邮件系统会按照事先设定好的内容自动给发信人回复一封确认收到的信件。但是，这个功能在给用户提供方便的同时，也有可能给用户制造邮件炸弹。这是因为如果发信人使用的邮件系统也开启了自动回复功能，而双方都没有及时看信的话，就会在反复“自动回信”中造就了一颗邮箱炸弹。
- 5. 指定邮件过滤规则**

用户可以利用邮箱的过滤器拦截恶意邮件，防止恶意邮件进入自己的邮箱。电子邮箱的过滤器可以为用户提供按照邮件的来源、接收者、主题等来设置过滤规则。通常某一类的恶

- 黑客
- 基础扫描
- 常用扫描
- 与嗅探工具
- 系统漏洞攻防
- 设置系统
- 安全策略
- 系统与文
- 件加密
- 远程控
- 制攻防
- 木马
- 聊天软
- 件攻防
- 网页恶意
- 代码攻防
- 电子邮
- 件攻防
- C盘病
- 毒攻防
- 使用电脑
- 安全软件
- 黑客技巧



意邮件是会有相关的主题字符的，如果不想再收到类似的恶意邮件，可以设置过滤在主题中有特定字符的邮件。

6. 限制接收邮件大小

如果黑客发送邮件炸弹不是大量的小型邮件，而是一封几百兆的“巨型炸弹”，一封邮件就会把用户的邮箱占满。因此，用户在设置邮件过滤规则的时候，需要格外注意“接收信件大小”选项，最好将这个数值控制在电子信箱的三分之一左右。例如，使用者的电子信箱空间是 30 MB，那么可以通过设置规定接收信件的大小不得超过 10 MB 每封，如果超过了这个数值，那么来信将被确认为邮件炸弹，而直接被系统舍弃，这样邮件炸弹便再无施展的空间了。

7. 使用转信功能

有些邮件服务器为了提高服务质量往往设有“自动转信”功能，利用该功能在一定程度上能够解决特大容量邮件的攻击。假设用户申请了一个转信信箱，利用该信箱的转信功能和过滤功能可以将那些不愿意看到的邮件统统过滤掉或者直接在邮件服务器中删除，也可以利用转信功能将垃圾邮件转移到不重要的信箱中。

8. 拒绝 Cookie 信息

许多网站会用不易察觉的技术，暗中搜集用户填写在表格中的电子邮件地址信息，最常见的就是利用 Cookie 记录访者的浏览行为和习惯。如果不想随便让 Cookie 来记录你的个人隐私信息，可以在浏览器中做一些设置，把 Cookie 功能屏蔽起来，这样浏览器在接受 Cookie 之前就会提醒用户，或者干脆拒绝它们。

10.5 防范电子邮件病毒

电子邮件病毒通常是把自己作为附件发送给被攻击者，如果接收到该邮件的用户不小心打开了附件，病毒即会感染你的电脑。对抗其中的病毒陷阱其实并不难，我们可以采取下面介绍的措施进行防范。

10.5.1 设置邮件的显示格式

由于 HTML 邮件具有可以嵌入 JavaScript 或是 VBScript 语句的特性，所以在收到的邮件中可能包含各种邮件病毒，或者收到存在恶意代码的 HTML 格式的邮件，让用户的电脑时刻暴露在危险的环境中。为了防范这些隐藏在电子邮件中的恶意代码和病毒，我们可以在收发邮件时将邮件的显示格式设置为纯文本，这样那些恶意代码和病毒就无法执行了。下面以 Outlook Express 接收邮件为例，介绍如何将邮件的显示格式设置为纯文本。

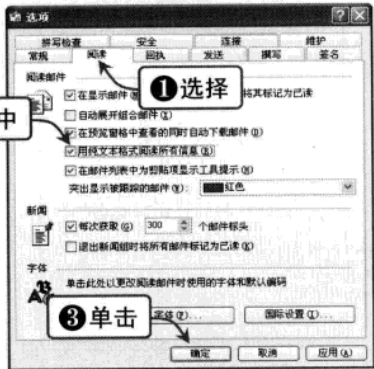
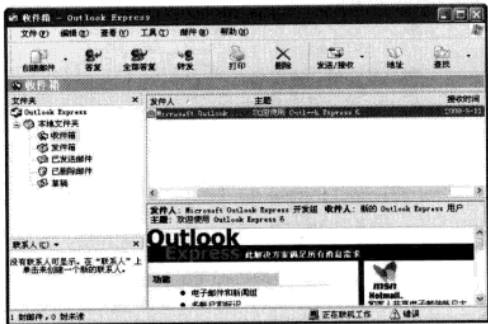
STEP 01 打开 Outlook Express

单击“开始”|“程序”|“附件”| Outlook Express 命令，启动 Outlook Express 程序，如下图所示。

STEP 02 设置邮件显示格式

单击“工具”|“选项”命令，在弹出的“选项”对话框中选择“阅读”选项卡，选中“用纯文本格式阅读所有信息”复选框，单击“确定”按钮，如下图所示。

Chapter 10 电子邮件攻防



10.5.2 设置 Outlook Express

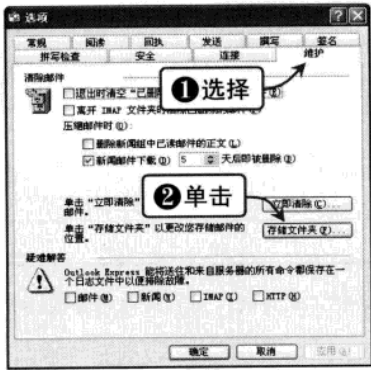
通过对 Outlook Express 进行一些具体的设置，也可以防止邮件病毒的攻击。

Work1 隐藏邮件文件夹

Outlook Express 泄密的关键在于存储邮件的文件夹被找到，导致攻击者可以随意窃取用户的邮件，窥探邮件中的重要信息。如果对存储邮件文件夹进行一些设置，那么安全系数会大大提高。下面将介绍一种隐藏存储邮件文件夹的方法。

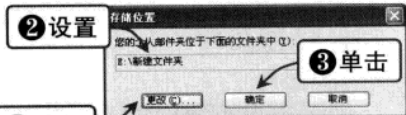
STEP 01 进入 Outlook Express 维护

运行 Outlook Express，在主窗口中单击“工具”|“选项”命令，在弹出的“选项”对话框中选择“维护”选项卡，单击“存储文件夹”按钮，如下图所示。



STEP 02 指定邮件文件存储路径

在弹出的“存储位置”对话框中单击“更改”按钮，指定存储邮件文件新的文件夹路径（本例中的存储路径为 E:\新建文件夹），单击“确定”按钮，如下图所示。当再次重新启动 Outlook Express 后，所有收发的邮件就会存放在新指定的文件夹下。



提示

指定的新文件夹建议放到 C 盘以外的地方，这样重新安装操作系统后个人邮件不会丢失。

STEP 03 隐藏文件夹

找到存储邮件文件的文件夹并右击，在弹出的快捷菜单中选择“属性”选项，在“常规”选项卡中选中“隐藏”复选框，单击“确定”按钮，如下图所示。

STEP 04 文件夹加密

使用 WinRAR 对文件夹进行压缩，压缩前选择“高级”选项卡，单击“设置密码”按钮，输入压缩密码，单击“确定”按钮即可，如下图所示。

黑客

常用扫描工具

系统漏洞扫描

设置系统安全策略

系统与文件加密

远程控制

木马攻击

聊天软件攻击

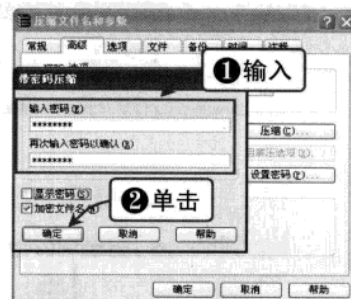
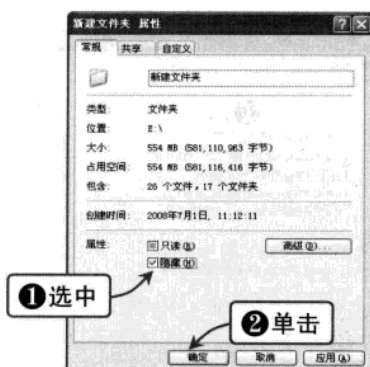
网页恶意代码攻击

电子邮件攻击

C 盘病毒攻击

使用电脑安全软件

黑客攻防实用技巧

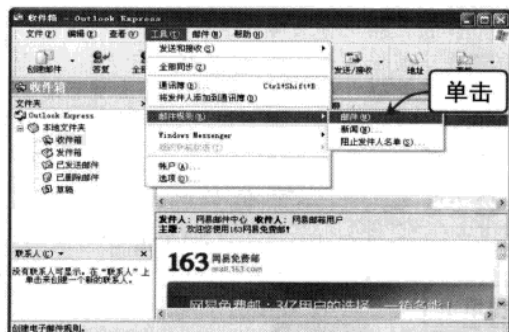


Work2 运用 Outlook Express 过滤器功能

如果用户不小心泄露或被黑客扫描到了自己的重要邮箱地址，很可能会收到带有病毒的电子邮件。利用 Outlook Express 自带的过滤器，用户可以根据需要设置一定的过滤规则，从而拒绝邮件病毒。Outlook Express 自带的规则条件有 12 种，下面就以过滤一个标题为 I love you 的爱虫病毒为例，进行具体设置。

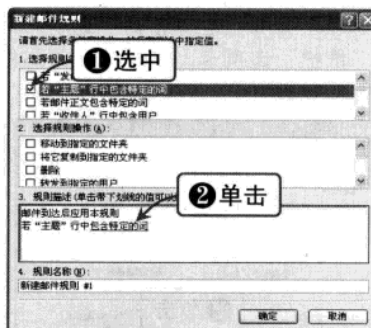
STEP 01 单击“邮件”命令

运行 Outlook Express，在主窗口中单击“工具”|“邮件规则”|“邮件”命令，如下图所示。



STEP 02 选择规则条件

弹出“新建邮件规则”对话框，在“1.选择规则条件”列表框中选中“若主题行中包含特定的词”复选框，在“规则描述”选项区中单击“包含特定的词”超链接，如下图所示。



提示

12 种规则条件是根据常见邮件病毒的特征制订的，用户可以根据实际情况进行具体选择。

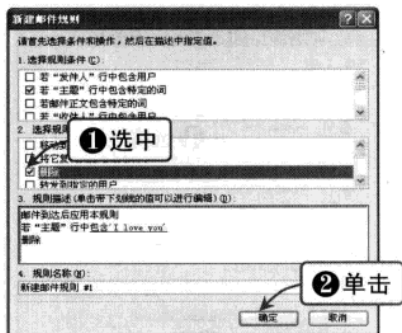
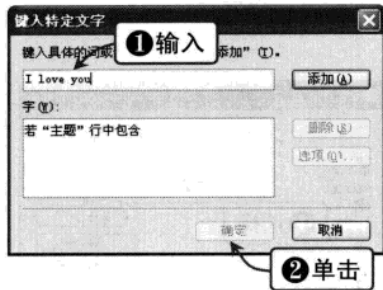
STEP 03 设置规则内容

弹出“键入特定文字”对话框，输入具体的词或句子，单击“添加”按钮，如有多个特定文字，可多次添加。添加完毕后，单击“确定”按钮，如下图所示。

STEP 04 选择规则操作

返回“新建邮件规则”对话框，在“2.选择规则操作”列表框中选择对符合规则的邮件要进行的操作。在此选中“删除”复选框，单击“确定”按钮，如下图所示。

Chapter 10 电子邮件攻防

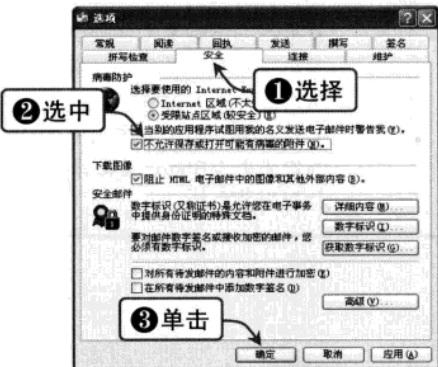


Work3 启动 Outlook Express 自动防毒功能

由于邮件病毒大多是通过加载邮件附件的方式进行传播的，所以可以使用禁止 Outlook Express 打开附件的方法防止此类病毒的侵害。同时，还可以禁止其他程序暗中利用用户的名义向别人发送邮件，具体设置方法如下：

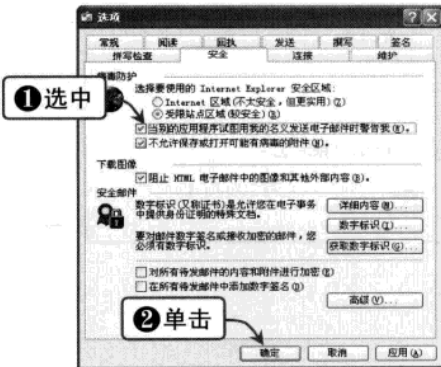
STEP 01 禁止打开病毒附件的设置

运行 Outlook Express，在主窗口中单击“工具”|“选项”命令，选择“安全”选项卡，在“病毒防护”选项区中选中“不允许保存或打开可能有病毒的附件”复选框，单击“确定”按钮，如下图所示。



STEP 02 禁止暗中发送邮件的设置

运行 Outlook Express，在主窗口中单击“工具”|“选项”命令，选择“安全”选项卡，在“病毒防护”选项区中选中“当别的应用程序试图用我的名义发送电子邮件时警告我”复选框，单击“确定”按钮，如下图所示。



10.5.3 变更文件关联

通过修改文件的关联属性，使得打开脚本文件时（例如，用户双击一个附件）不会像原来那样自动运行，而是用记事本打开并处于编辑状态。这样，就可以防止蠕虫病毒通过.vbs等格式的邮件附件传播，减少这类病毒带来的风险。

STEP 01 打开文件夹选项

单击“开始”|“设置”|“控制面板”命令，并打开“文件夹选项”对话框，在“已注册的文件类型”列表框中选择 VBS 扩展名选项，单击“高级”按钮，如下图所示。

STEP 02 编辑文件类型

弹出“编辑文件类型”对话框，在“操作”选项区中选择“编辑”选项，单击“编辑”按钮，如下图所示。

基础知识
黑客
常用扫描
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统安全
加密
远程控制
木马
聊天软
件攻防
网页恶
意代码防
电子邮
件攻防
C盘病
使用电
脑安全
黑客攻
防技巧



11.1 U 盘病毒概述

U 盘病毒又称为 autorun 病毒，是依托 U 盘、移动硬盘等移动存储设备，通过名为 autorun 的隐藏文件进行传播的，后缀名通常为 inf、exe 等几种。U 盘病毒不但扰乱了电脑操作系统的正常使用，非法篡改、删除用户数据资料，而且可能会造成大规模的病毒扩散等现象。

11.1.1 U 盘病毒的原理和特点

要研究 U 盘病毒，首先要了解它的原理和特点。

Work1 U 盘病毒的原理

U 盘病毒利用了 autorun.inf 自动运行的原理进行传播。病毒首先向 U 盘写入病毒程序，然后更改 autorun.inf 文件。Windows 运行被更改的 autorun.inf 文件就会激活病毒。被激活的 U 盘病毒还会自动检测新插入的 U 盘，进行自身的复制和传播。

Work2 U 盘病毒的特点

当用户在使用 U 盘等移动存储设备的过程中，发现打开 U 盘时速度极慢，双击进入时总是显示被某程序占用之类的提示；或在 U 盘右键菜单中出现“自动播放”、Auto 等选项时，则表明用户已经感染 U 盘病毒。

U 盘病毒发作时具有以下特性：

- ❖ 传播速度快：由于 U 盘病毒能够自动执行，在用户电脑系统没有采取防护措施的情况下，往往在病毒 U 盘插入 USB 接口的一瞬间，即已感染病毒。
- ❖ 隐蔽性高：U 盘病毒本身是以“隐藏文件”的形式存在的，而且能伪装在其他正常系统文件夹和文件中，不易被察觉。
- ❖ 传播范围广：随着 U 盘、移动硬盘等移动存储设备的大量普及，就会造成大规模的病毒扩散现象。

11.1.2 常见 U 盘病毒

利用 autorun.inf 自动运行的原理，U 盘病毒的数量与日俱增，下面将简单介绍几种常见的 U 盘病毒。

Work1 Adober.exe 病毒

当用户的操作系统感染 Adober.exe 病毒后，双击 U 盘时暂无反映。等一会儿就会弹出对话框“Adober.exe error，请查看 Adober.exe.log”，并且 U 盘根目录中多了一个 Adober.exe 文件，其图标为一个普通可执行程序。

当右击 U 盘时，在快捷菜单最上面出现 Auto 这一选项。同时，查看任务管理器时会发现进程中出现名为 Adober.exe 的进程，电脑速度缓慢。

该病毒是检测到有 U 盘插入后，自动从感染主机中复制 Adober.exe 和自动启动文件 autorun.inf，使得 U 盘图标在被双击后，执行 Adober.exe，吞噬系统的内存（每次双击，进

Chapter 11 U 盘病毒攻防

程中都会多一个 Adober.exe)，并修改注册表，在系统盘中自我备份，以感染更多的插往该主机上的 U 盘。

Work2 sxs.exe 病毒

当用户的操作系统感染 sxs.exe 病毒后，单击电脑上各个磁盘分区时，均无反应，只能通过右键快捷菜单中的“打开”选项打开，且在右键菜单里新增了“自动播放”选项。每个磁盘分区（除了 C 盘）都有 autorun.inf 和 sxs.exe 两个文件，删除之后会再生。

U 盘无法进行“安全删除”，显示无法停止的对话框。

某些杀毒软件实时监控自动关闭，并无法打开。

查看任务管理器时，就会发现进程中出现名为 sxs.exe 或 svohost.exe 的进程。

Work3 doc.exe 病毒

当用户把染有该病毒的 U 盘插入后，操作系统中即被写入 win32.exe、win33.exe 以及很多.exe 的病毒文件，以相似图标冒充 MP3 和 DOC 文档。该病毒一旦发作，可以将 Office 用户的 Word 文档逐个删除，所有 Windows 版本用户无一幸免。

查看任务管理器时，就会发现进程中出现名为 doc.exe 的进程。

Work4 RavMone.exe 病毒

RavMone.exe 企图冒充瑞星杀毒软件的正常文件 RavMon.exe 和 RavMond.exe。当用户双击 U 盘盘符时，就会激活 autorun.inf 自动加载 RavMone.exe。

中毒之后，电脑识别 U 盘时会出现一些问题，双击打开十分缓慢；查看所有文件，发现多了 RavMone.exe、RavMonLog、msvcr71.dll 等几个文件。且 U 盘无法正常退出，病毒又会传染给新的 U 盘。同时，还会在各个磁盘分区中生成 RavMone.exe.log 文件，删除之后会再生。



提示

新的 U 盘病毒层出不穷，但其原理基本都是一样的，只要用户平时使用电脑时细心一些，就不难发现它们。

11.2 U 盘病毒的防御

为了保证用户电脑系统的良好运行，就要针对 U 盘病毒采取一系列的防御措施，主要措施有：关闭系统默认打开的“自动播放”功能，在日常的生活和学习中养成良好的安全使用 U 盘习惯等。

11.2.1 使用组策略关闭“自动播放”功能

有以下几种方法可以关闭“自动播放”功能，使用组策略的操作方法如下：

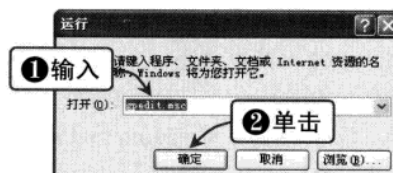
STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，如下图所示。

STEP 02 输入命令

在弹出的“运行”对话框中输入 gpedit.msc 命令，单击“确定”按钮，如下图所示。

基础知
黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码防
电子邮
件攻防
C 盘病
毒攻防
使用电
脑安全软
件
黑客攻
防实用技
巧

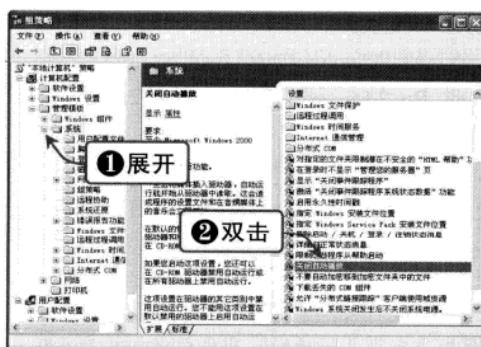


STEP 03 关闭“自动播放”选项

在“组策略”窗口的左窗格中依次打开“电脑配置\管理模板\系统”分支，在右窗格的“设置”列表框中双击“关闭自动播放”选项，如下图所示。

STEP 04 关闭“自动播放”属性

在“关闭自动播放属性”对话框中，选中“已启用”复选框，单击“确定”按钮，如下图所示。



11.2.2 修改注册表关闭“自动播放”功能

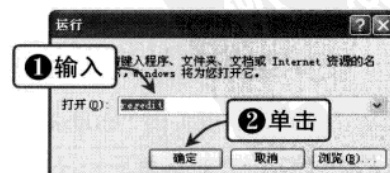
通过修改注册表也可以关闭“自动播放”功能，具体操作步骤如下：

STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，如下图所示。

STEP 02 输入命令

在弹出的“运行”对话框中输入 regedit 命令，单击“确定”按钮，如下图所示。



Chapter 11 U 盘病毒攻防

STEP 03 打开注册表编辑器

在“注册表编辑器”左窗格中依次打开 HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2 分支并右击，在弹出的快捷菜单中选择“权限”选项，如下图所示。



STEP 04 设置用户权限

在弹出的“MountPoints2 的权限”对话框中单击 Administrator 用户，在“Administrator 的权限”选项区中选中所有的“拒绝”复选框，单击“确定”按钮，如下图所示。

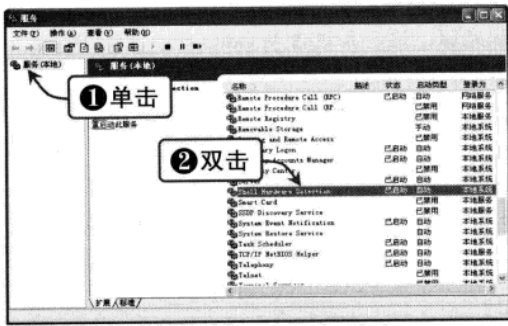


11.2.3 设置服务关闭“自动播放”功能

停止相关系统服务也可以关闭“自动播放”功能，具体操作步骤如下：

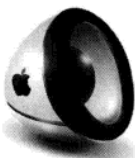
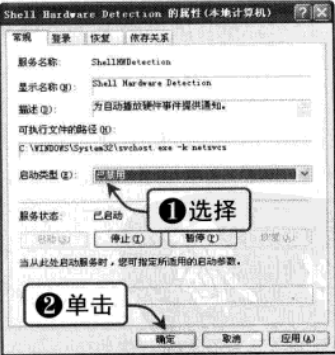
STEP 01 打开“服务”窗口

单击“开始”|“控制面板”|“管理工具”|“服务”命令，双击 Shell Hardware Detection 选项，如下图所示。



STEP 02 设置 Shell Hardware Detection 服务属性

弹出“Shell Hardware Detection 属性”对话框，在“启动类型”下拉列表框中选择“已禁用”选项，单击“确定”按钮，如下图所示。



提示

在 U 盘的根目录下建立 Autorun.inf 目录，并设其属性为“隐藏”和“只读”，可以截断利用移动磁盘自运行进行传播的病毒。建议所有的磁盘根目录下都建立此目录。

黑客
常用扫描
漏洞攻防
安全策略
系统与安全
远程控制
木马
聊天软件
网页恶意
电子邮件
病毒攻防
使用电脑
黑客技巧



11.2.4 使用安全的操作方法

为了避免 U 盘病毒的感染，应使用以下安全的操作方法：

- ❖ 有写保护功能的 U 盘要充分使用写保护功能，在插入不安全的电脑前要打开写保护功能，防止感染病毒。
- ❖ 使用 U 盘等移动存储设备时，务必要做到先查毒后打开。
- ❖ 插入 U 盘后，不要双击打开 U 盘，应使用右键快捷菜单中的“打开”选项打开 U 盘，很多时候可以避免 U 盘中的 autorun.inf 文件被运行。

11.3 autorun.inf 解析

绝大部分 U 盘病毒都是通过 autorun.inf 的自动播放功能引发病毒感染的，因此了解 autorun.inf 文件的构造和运行机制是很有必要的。

Work1 autorun.inf 文件简介

autorun.inf 文件是一种具有特定结构的必须放在驱动器根目录下的文件，它控制着双击驱动器时的自动播放选项。U 盘病毒的传播基本上都借助了 autorun.inf 文件，电脑上的病毒首先将自身复制到已连接的 U 盘上，然后创建一个 autorun.inf 文件，当此 U 盘接入到其他电脑上以后，在用户双击 U 盘时系统就会根据 U 盘里 autorun.inf 文件中的设置去运行 U 盘的病毒或者指定的程序，导致系统出现各种非正常症状，如磁盘无法打开，系统死机等。

Work2 autorun.inf 文件的构造

autorun.inf 文件是从 Windows 95 开始存在的，最初用在其安装盘中实现自动安装，以后的各版本都保留了该文件部分内容，也可用于其他存储设备。

autorun.inf 文件结构有三个部分：

- ❖ [AutoRun] 适用于 Windows 95 以上系统与 32 位以上 CD-ROM，必选。
- ❖ [AutoRun.alpha] 适用于基于 RISC 的电脑光驱，适用系统为 Windows NT 4.0，可选。
- ❖ [DeviceInstall] 适用于 Windows XP 以上系统，可选。

一般用户所见到的 autorun.inf 文件只保留了 [AutoRun] 小节。

下表列出了 U 盘病毒 autorun.inf 文件 [AutoRun] 小节的内容：

[AutoRun]	//表示 AutoRun 部分开始
Icon=X:\“图标”.ico	//给 X 盘一个图标
Open=X:\“程序”.exe 或者“命令行”	//双击 X 盘执行的程序或命令
Shell\“关键字”=“鼠标右键菜单中加入显示的内容”	//右键菜单新增选项
Shell\“关键字”\command=“要执行的文件或命令行”	//选中右键菜单新增选项执行的程序或者命令

Work3 autorun.inf 文件的编写

下面通过一个简单实例来编写一个 autorun.inf 文件，假设 U 盘根目录下有 ABC.ico、ABC.exe、ABC.txt 三个文件。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

打开记事本程序，输入以下内容：

```
[AutoRun]
Icon=ABC.ico
Open=ABC.exe
shell\1=打开 ABC.txt
shell\1\command=notepad ABC.txt
```

然后保存该文本名字为 autorun.inf，当系统寻找到 autorun.inf 以后，U 盘图标就会显示为 ABC.ico，双击便会执行 ABC.exe，当右击 U 盘图标时，在快捷菜单中就多出一个“打开 ABC.txt”选项，选择它就会用系统自带的 notepad（记事本）程序打开 ABC.txt。

11.4 U 盘病毒的查杀

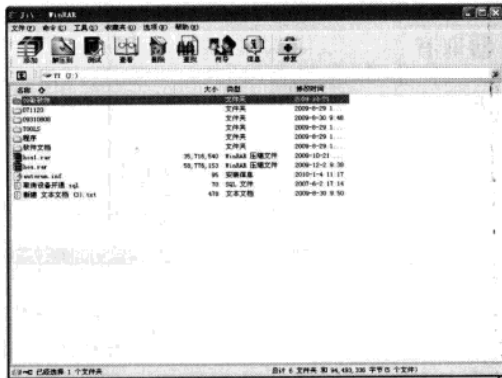
U 盘病毒查杀的主要方法有：利用 WinRAR 查杀、手工查杀和利用 U 盘病毒专杀软件进行查杀。下面将具体介绍这几种查杀方式。

11.4.1 用 WinRAR 查杀 U 盘病毒

一般的 U 盘病毒文件具有隐蔽性, 在 Windows 正常状态下是无法查看的。而利用 WinRAR 则可以查看隐藏的 U 盘病毒文件。具体操作步骤如下:

STEP 01 通过 WinRAR 软件打开 U 盘

运行 WinRAR 软件，选择路径下拉菜单中的 U 盘位置，查看 U 盘根目录中的文件，如下图所示。

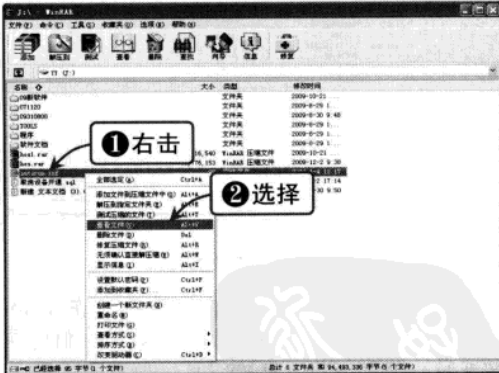


STEP 03 查看文件内容

在 WinRAR 的查看窗口中查看文件内容，如果显示内容中有一行为：“open=***.exe”，则可判定已经感染病毒，关闭查看窗口，如下图所示。

STEP 02 找到可疑文件或文件夹

在 U 盘根目录中查看是否有 autorun.inf 文件, 如果有, 则右击此文件, 在弹出的快捷菜单中选择“查看文件”选项, 如下图所示。



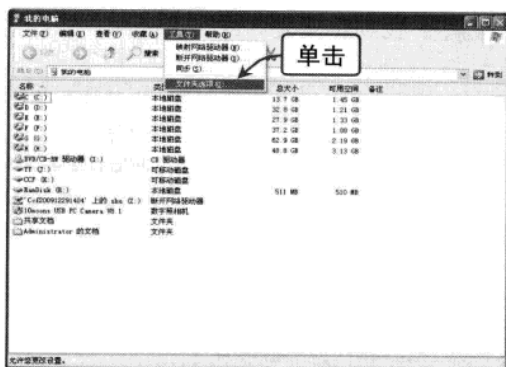
STEP 04 删除病毒文件

在 WinRAR 窗口中右击 autorun.inf 文件，在弹出的快捷菜单中选择“删除文件”选项，即可删除文件，如下图所示。



使用显示系统隐藏文件的方法可以手工进行 U 盘病毒的判断删除, 具体操作步骤如下:

在“我的电脑”窗口中，单击“工具”|“文件夹选项”命令，如下图所示。

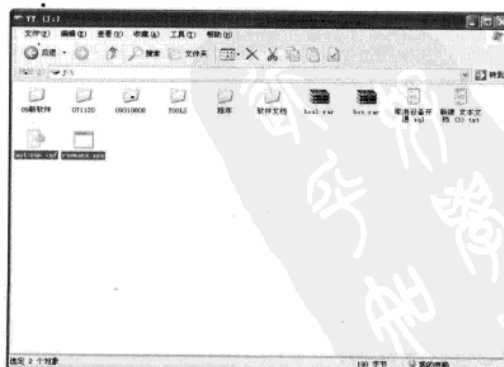
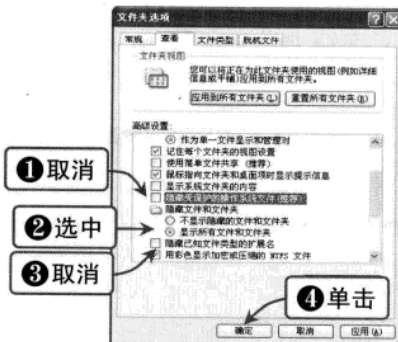


打开 U 盘根目录，查看是否存在 auto-run.info、msvcr71.dl、ravmone.exe 等类似的异常文件，如果有将其删除即可，如右图所示。



在 U 盘根目录默认正常状态下是没有隐藏文件的, 如果发现有, 那就要小心查看了, 十有八九就是中招了!

在弹出的“文件夹选项”对话框中取消选择“隐藏受保护的操作系统文件”复选框，选中“显示所有文件和文件夹”单选按钮，取消选择“隐藏已知文件类型的扩展名”复选框，单击“确定”按钮，如下图所示。



Chapter 11 U 盘病毒攻防

11.4.3 U 盘病毒专杀工具——USBCleaner

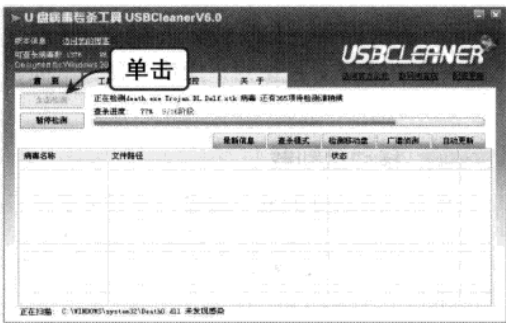
USBCleaner 是一款纯绿色的辅助杀毒工具，其最新版支持简体中文与繁体中文切换，支持 Vista，独有的分类查杀引擎能检测查杀 1 300 余种 U 盘病毒，具有 U 盘病毒广谱扫描、U 盘病毒免疫、修复显示隐藏文件及系统文件、安全卸载移动盘盘符等功能，能全方位一体化查杀 U 盘病毒。

Work1 USBCleaner 全面检测

最新的 USBCleaner 全面检测可精确查杀已知的 1376 种 U 盘病毒，并修复这些 U 盘病毒对系统的破坏。全面检测分为 16 个阶段，检测完毕后将自动进入广谱深度检测阶段。

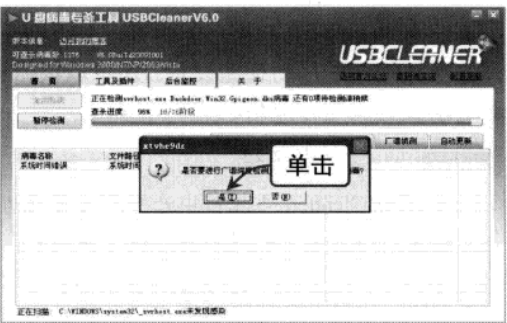
STEP 01 进行全面扫描

在 USBCleaner 主界面中选择“首页”选项卡，单击“全面检测”按钮，开始对用户电脑进行全面扫描，如下图所示。



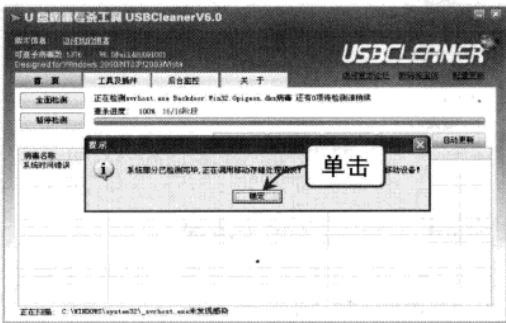
STEP 02 选择广谱扫描

全面检测完毕后，弹出提示信息框，单击“是”按钮，开始进行广谱扫描，如下图所示。



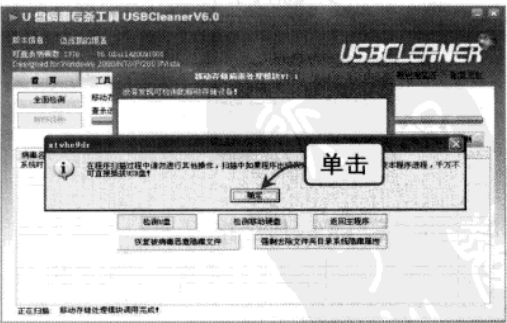
STEP 03 系统检测完毕

系统部分检测完毕后，弹出提示信息框，插入移动存储设备后单击“确定”按钮，如下图所示。



STEP 04 准备检测 U 盘

单击“检测 U 盘”按钮，弹出提示信息框，单击“确定”按钮，如下图所示。



基础知识

常用扫描与嗅探工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文

远程攻击

木马

聊天软件

网页攻击

代码攻击

电子战

黑客攻防

使用电脑

黑客技巧



STEP 05 开始检测 U 盘

当软件检测到 U 盘后，会弹出提示信息框。单击“确定”按钮后开始检测移动存储设备，如下图所示。



STEP 06 U 盘检测完毕

U 盘检测完毕后弹出提示信息框，单击“确定”按钮，显示本次检测结果。

单击“恢复被病毒恶意隐藏文件”按钮，可对已隐藏文件进行修复，如下图所示。

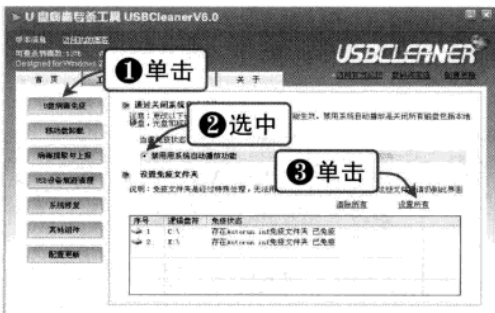


Work2 USBCleaner 工具及插件

USBCleaner 具有简单、时尚的工具界面，全面的防杀模块，有效的防杀能力，可以全方位一体化保护移动存储设备。还可以根据用户需求自由选择工具按钮，操作方便。下面将对其主要功能进行介绍。

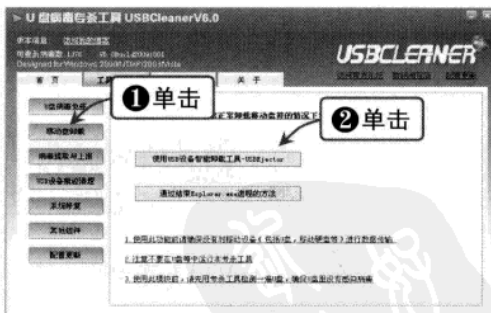
STEP 01 U 盘病毒免疫

在 USBCleaner 主界面中选择“工具及插件”选项卡，单击“U 盘病毒免疫”按钮。选中“禁用系统自动播放功能”单选按钮，单击“设置所有”超链接，即关闭了系统的自动播放功能，并对用户电脑内各个分区添加免疫目录，如下图所示。



STEP 02 移动盘卸载

单击“移动盘卸载”按钮，当用户不能正常卸载移动盘符的情况下，通过单击两种方式按钮，可安全、有效地卸载移动盘符，如下图所示。



STEP 03 病毒提取与上报

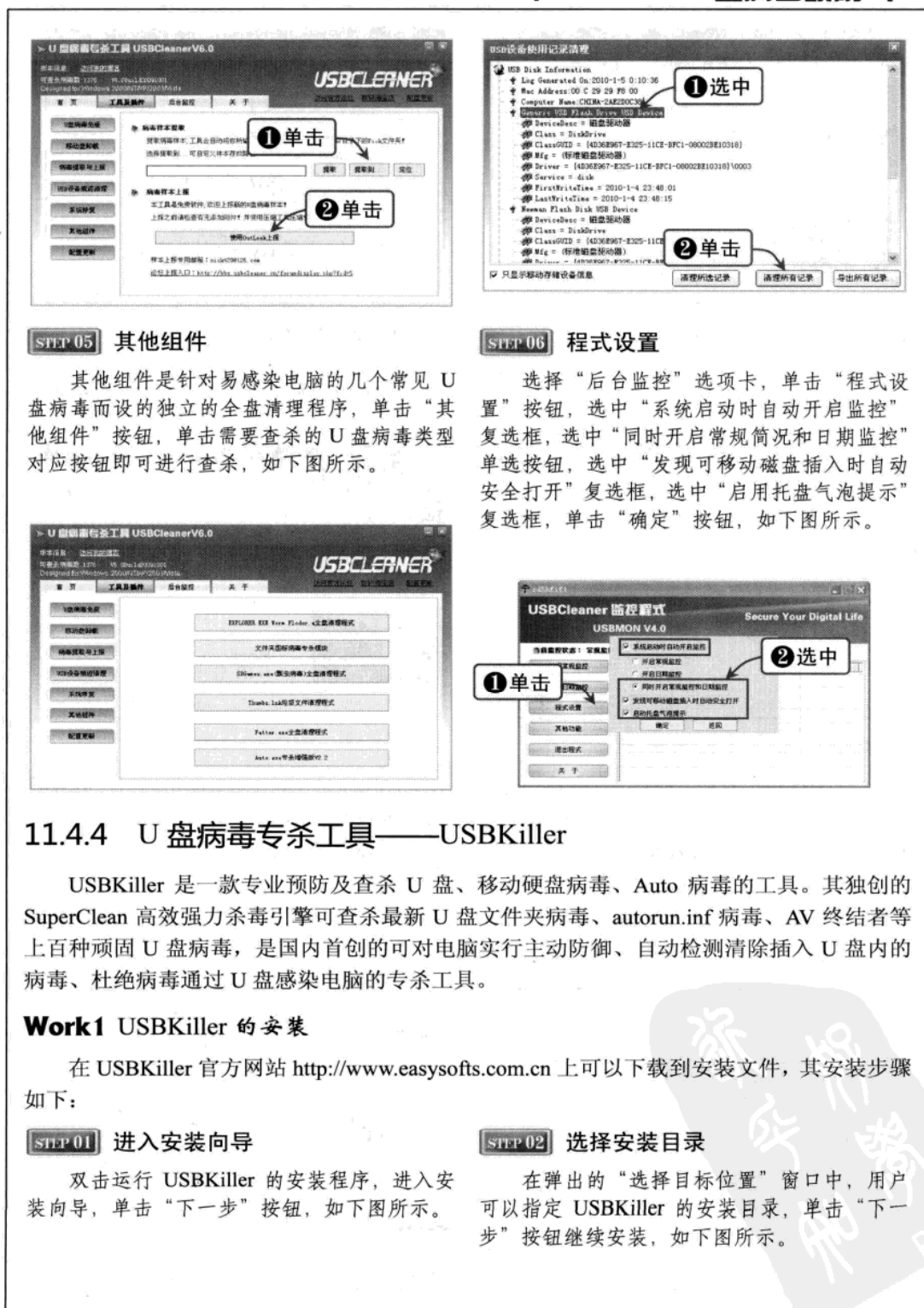
USBCleaner 提供专门的病毒提取工具，帮助用户安全地提取病毒样本上报给官方，帮助官方完善 USBCleaner。单击“提取到”按钮，选择样本位置。单击“使用 Outlook 上报”按钮进行病毒样本上报传送，如下图所示。

STEP 04 USB 设备痕迹清理

单击“USB 设备痕迹清理”按钮，在弹出的“USB 设备使用记录清理”对话框中选中需要清理的对象，单击“清理所选记录”按钮进行清除。也可单击“清理所有记录”按钮，即可清理列表框中所有记录，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 11 U 盘病毒攻防



U 盘数据清理工具 USBCleaner V6.0

版本信息: 2012.07.26 22:00
 可搜索到硬盘: 1275 MB, 100% (2008.08.01)
 Designed for Windows 2000/XP/Vista/7/8/8.1

主 页 工具及插件 功能介绍 关于

1 单击

2 单击

程序主程序路径: c:\program files\usb cleaner\usb cleaner.exe
 论坛主入口: http://www.ahzhong.com/forum.php?mod=viewthread

STEP 05 其他组件

其他组件是针对易感染电脑的几个常见 U 盘病毒而设的独立的全盘清理程序, 单击“其他组件”按钮, 单击需要查杀的 U 盘病毒类型对应按钮即可进行查杀, 如下图所示。



USB设备使用记录清理

USB Disk Information

Log Generated On: 2010-1-5 0:10:36

Mac Address: 00 C 29 29 F9 00

Computer Name: CHINA-2A220C00

General USB Flash Drive Info

DeviceBase = 磁盘驱动器

Class = DiskDrive

ClassGUID = {4362A67F-E305-11CF-BFC1-080023E10318}

Mfg = (待清理磁盘驱动器)

Driver = {4362A67F-E305-11CF-BFC1-080023E10318}\Voodoo

Service = disk

FirstWriteTime = 2010-1-4 23:48:01

LastWriteTime = 2010-1-4 23:48:15

Remove Flash Disk Info

DeviceBase = 磁盘驱动器

Class = DiskDrive

ClassGUID = {4362A67F-E305-11CF-BFC1-080023E10318}

Mfg = (待清理磁盘驱动器)

DeviceName = {F8000000-0000-0000-0000-000000000000}

1. 选中

2. 单击

☒ 只清理移动存储设备信息

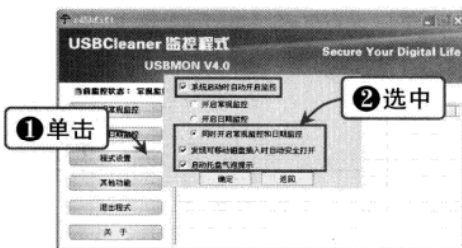
清理所选记录

清理所有记录

导出所有记录

STEP 06 程式設置

选择“后台监控”选项卡，单击“程式设置”按钮，选中“系统启动时自动开启监控”复选框，选中“同时开启常规简况和日期监控”单选按钮，选中“发现可移动磁盘插入时自动安全打开”复选框，选中“启用托盘气泡提示”复选框，单击“确定”按钮，如下图所示。



11.4.4 U 盘病毒专杀工具——USBKiller

USBKiller 是一款专业预防及查杀 U 盘、移动硬盘病毒、Auto 病毒的工具。其独创的 SuperClean 高效强力杀毒引擎可查杀最新 U 盘文件夹病毒、autorun.inf 病毒、AV 终结者等上百种顽固 U 盘病毒，是国内首创的可对电脑实行主动防御、自动检测清除插入 U 盘内的病毒、杜绝病毒通过 U 盘感染电脑的专杀工具。

Work1 USBKiller 的安装

在 USBKiller 官方网站 <http://www.easysoft.com.cn> 上可以下载到安装文件，其安装步骤如下：

STEP 01 进入安装向导

双击运行 USBKiller 的安装程序，进入安装向导，单击“下一步”按钮，如下图所示。

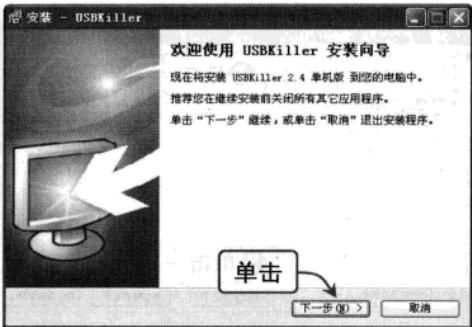
STEP 02 选择安装目录

在弹出的“选择目标位置”窗口中，用户可以指定 USBKiller 的安装目录，单击“下一步”按钮继续安装，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

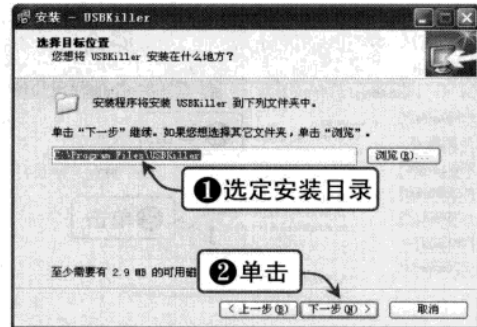
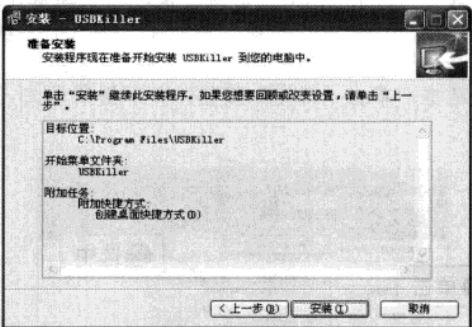


黑客攻防从新手到高手



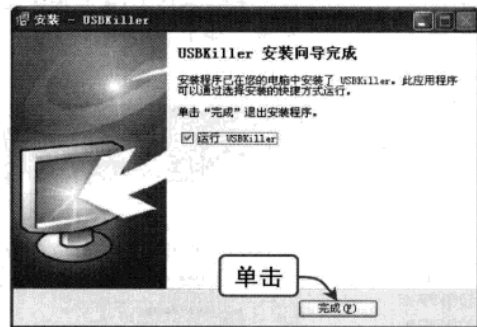
STEP 03 确定安装信息

在“准备安装”窗口中显示了安装目录和附加任务列表。确认无误后，单击“安装”按钮继续安装，如下图所示。



STEP 04 完成程序安装

依次单击“下一步”按钮继续安装，当出现完成窗口时，单击“完成”按钮完成安装，如下图所示。

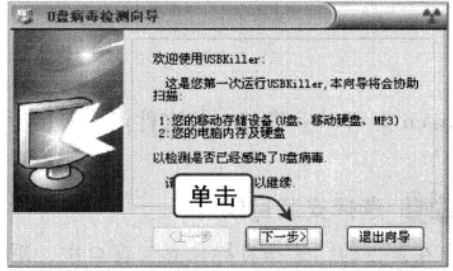


Work2 U 盘病毒检测向导

在 USBKiller 安装完成后，就会自动进入 U 盘病毒检测向导窗口，自动扫描用户电脑的移动设备、内存和硬盘，查出可疑病毒等。具体操作步骤如下：

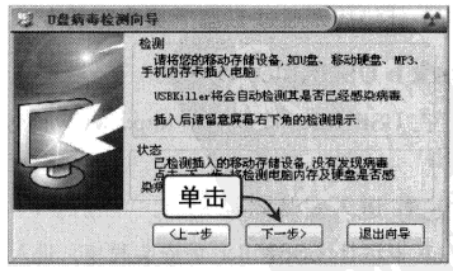
STEP 01 进入病毒扫描向导

在初次运行 USBKiller 时，将进行病毒检测扫描。单击“下一步”按钮继续，如下图所示。



STEP 02 检测移动设备

USBKiller 自动检测用户电脑中插入的移动设备。检测完毕后显示检测结果。单击“下一步”按钮继续，如下图所示。



STEP 03 检测硬盘

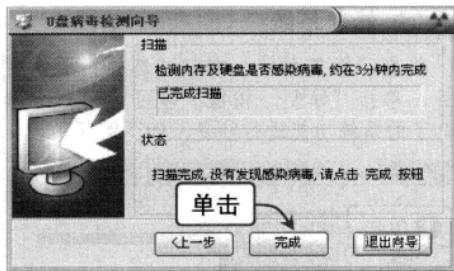
USBKiller 自动扫描用户电脑的内存和硬盘，实时显示状态，如下图所示。

STEP 04 扫描完成

扫描完成后，将会显示扫描结果。单击“完成”按钮完成检测向导，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 11 U 盘病毒攻防

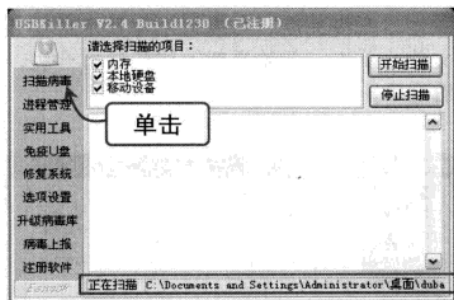


Work3 USBKiller 功能介绍

USBKiller 除了 U 盘病毒扫描功能外，还具有检测进程管理、自动建立免疫目录、解锁 U 盘等安全实用的功能，其使用界面简单，功能更完善。

STEP 01 扫描病毒

单击“扫描病毒”按钮，选择需要扫描的项目，单击“开始扫描”按钮；扫描进度在窗口下方显示。如果发现病毒，软件会自动进行清除操作，如下图所示。



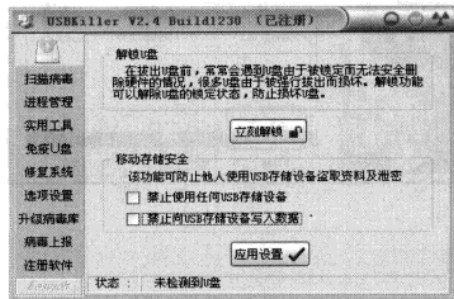
STEP 02 进程管理

单击“进程管理”按钮，可以查看运行的所有进程。选中“进程名称”复选框，单击“终止”按钮，可以停止所选进程，如下图所示。



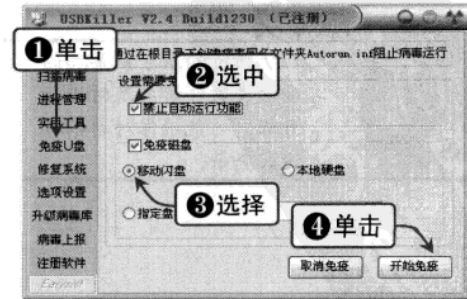
STEP 03 实用工具

单击“实用工具”按钮，单击“立即解锁”按钮，可以安全地退出被锁定的移动设备；为防止使用移动存储设备盗取资料，可选中“禁止向 USB 存储设备写入数据”复选框，单击“应用设置”按钮，如下图所示。



STEP 04 免疫 U 盘

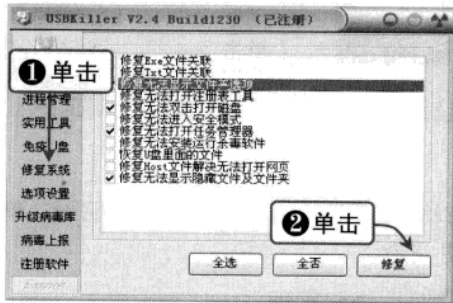
单击“免疫 U 盘”按钮，选中“禁止自动运行功能”复选框，选中“移动闪存”单选按钮，单击“开始免疫”按钮，则在用户的移动存储设备中建立了免疫目录，如下图所示。





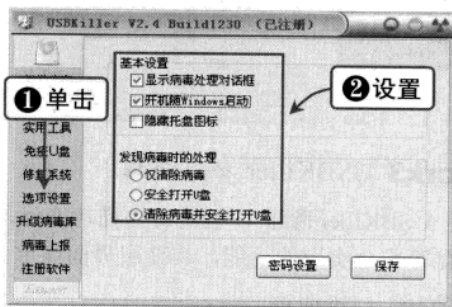
STEP 05 修复系统

单击“修复系统”按钮，选择需要修复的项目，单击“修复”按钮，即可对被U盘病毒破坏了的系统功能进行修复，如下图所示。



STEP 06 选项设置

单击“选项设置”按钮，可设置软件的基本属性及对病毒的处理方式，如下图所示。

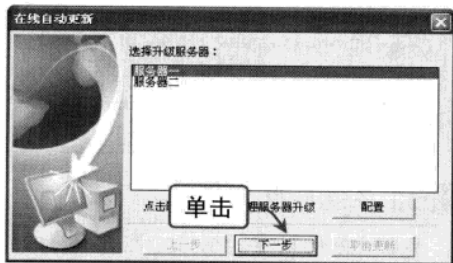


Work4 升级病毒库

用户应该定时更新病毒库，防止新型U盘病毒的入侵，具体操作步骤如下：

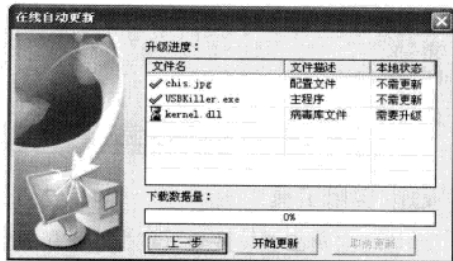
STEP 01 准备升级

在保证互联网连通的情况下，单击“升级病毒库”按钮，进入“在线自动更新”对话框，选择升级服务器，单击“下一步”按钮，如下图所示。



STEP 02 升级进程

在“升级进度”列表框中会显示需要升级的文件，单击“开始更新”按钮进行升级，如下图所示。



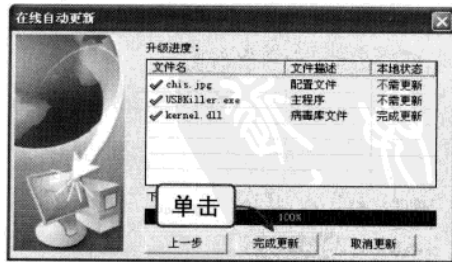
STEP 03 升级完成

升级完毕后，单击“完成更新”按钮即可，如右图所示。



提示

所有的基于病毒库的安全类软件都要及时进行升级，才能确保对新病毒进行查杀。



Chapter

12

使用电脑安全软件

常用的电脑安全软件包括杀毒软件和网络防火墙两种。杀毒软件也叫反病毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件的一类软件。杀毒软件通常集成病毒监控、病毒扫描和清除以及自动升级等功能。网络防火墙可以是一台专属的硬件或是架设在硬件上的一套软件，本书介绍的防火墙特指软件防火墙。本章将详细介绍几种常见的杀毒软件和防火墙软件的使用方法。

本章建议学习时间：

本章建议学习时间为 70 分钟，其中分配 40 分钟学习杀毒软件和防火墙应用的相关知识，30 分钟观看教学视频并进行练习。

学完本章后您可以：

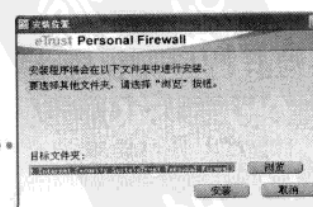
- 使用杀毒软件清除电脑病毒
- 使用常见杀毒软件
- 学会清理电脑中的恶意软件
- 使用防火墙抵御网络攻击
- 使用常见网络防火墙



选择手动扫描的方式



标准扫描



设置安装位置

重要知识点视频索引



12.1 使用杀毒软件清除电脑病毒

用户在使用电脑时经常会因为各种各样的原因导致电脑感染病毒。在电脑中毒后，就会引起系统变慢、频繁死机等问题，这时就需要使用杀毒软件清除电脑病毒。常见的杀毒软件有金山毒霸、卡巴斯基、瑞星、NOD32、Norton AntiVirus 等，下面将分别进行介绍。

12.1.1 金山毒霸的使用

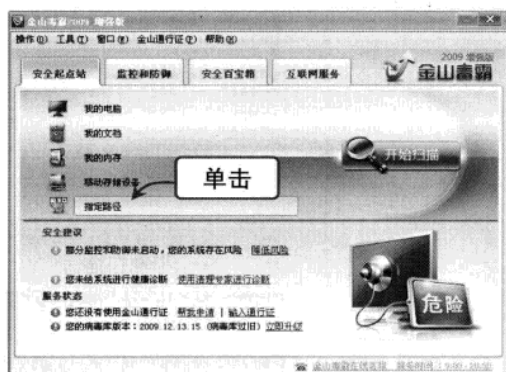
金山毒霸是金山软件公司推出的智能反病毒软件，是市场上较有影响力的一个品牌，特别是其通过了多项国际杀毒认证和 Windows Vista 官方认证，更增强了产品在市场的竞争力。金山毒霸官方网站地址为 <http://www.duba.net>。金山毒霸具有查杀病毒和病毒监控的功能，其中查杀病毒的方式主要有两种：手动查杀和定时查杀。

Work1 手动查杀病毒

在用户电脑已经感染病毒的情况下，一般直接采取手动查杀的方式。使用手动查杀病毒的具体操作步骤如下：

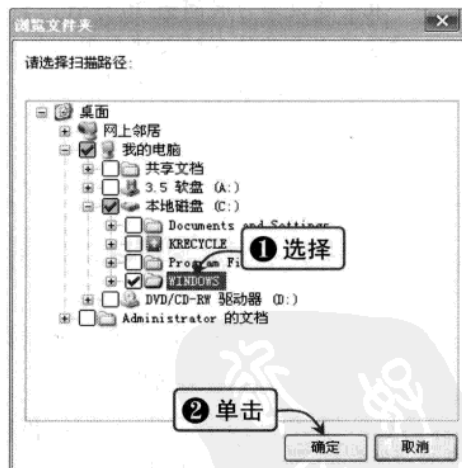
STEP 01 选择手动扫描的方式

金山毒霸对于手动查杀提供了几种扫描方式：我的电脑、我的文档、我的内存、移动存储设备、指定路径。下面以指定路径为例进行介绍，单击“指定路径”按钮，如下图所示。



STEP 02 选择路径

在弹出的“浏览文件夹”对话框中，依次展开“本地磁盘 (C:) \WINDOWS”分支，选择需要扫描的文件或文件夹，单击“确定”按钮后，即开始扫描病毒，如下图所示。



STEP 03 扫描病毒

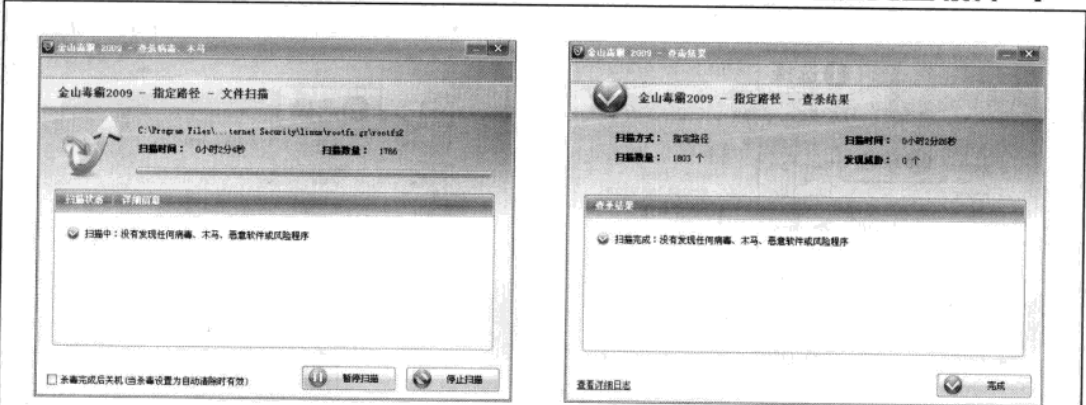
在扫描过程中，软件会实时显示扫描时间、扫描数量、扫描状态及详细信息等，如下图所示。

STEP 04 扫描完成

扫描完成后，在查毒结果窗口会以列表方式显示查杀结果，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件

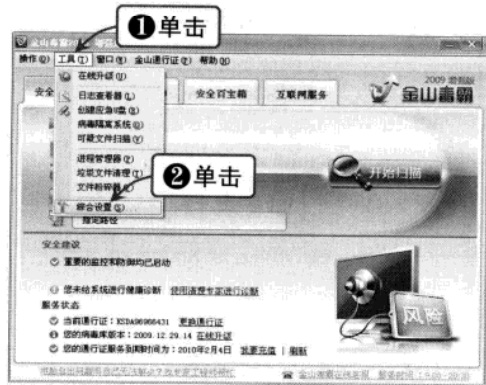


Work2 定时查杀病毒

使用“定时杀毒”功能可以自动执行用户事先定制好的查杀任务，达到事半功倍的效果。定时查杀病毒的具体操作步骤如下：

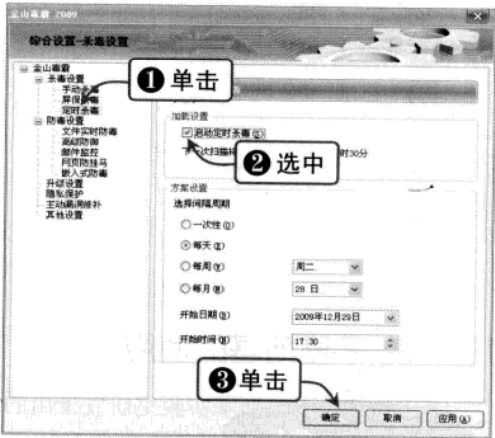
STEP 01 打开定时查杀的设置

在金山毒霸 2009 主界面菜单栏中单击“工具”|“综合设置”命令，如下图所示。



STEP 02 定时杀毒设置

在杀毒设置对话框中，单击“定时杀毒”选项后，选中“启动定时杀毒”复选框，便可根据用户需要设置不同的间隔周期，单击“确定”按钮，如下图所示。



Work3 监控与防御

金山毒霸还为用户提供了实时的监控与防御功能。使用实时监控与防御功能的具体操作步骤如下：

STEP 01 启动和关闭监控与防御

在金山毒霸 2009 主界面中选择“监控和防御”选项卡，单击“关闭”或“启动”按钮即可随时关闭或启动相应的功能，如下图所示。

STEP 02 文件实时防毒设置

在“工具”|“高级设置”中，选择“文件实时防毒”选项，可对其进行具体设置，单击“确定”按钮，如下图所示。

基础知识

常用扫描工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制攻防

木马攻击

聊天软件攻防

网页恶意代码攻防

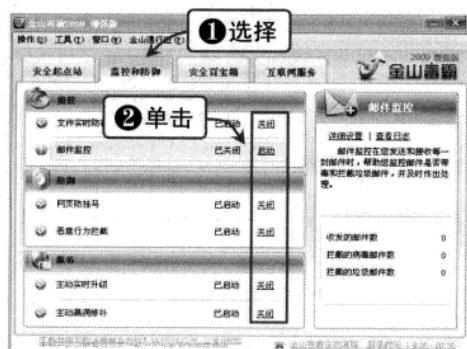
电子邮件攻防

病毒攻防

使用电脑安全软件

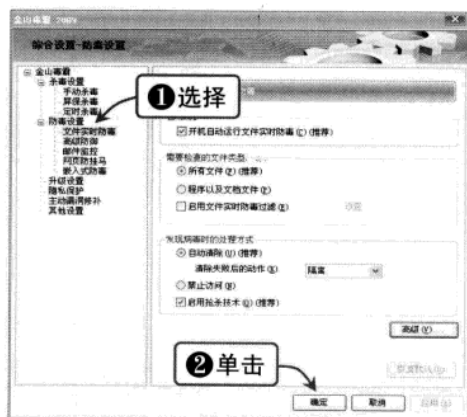
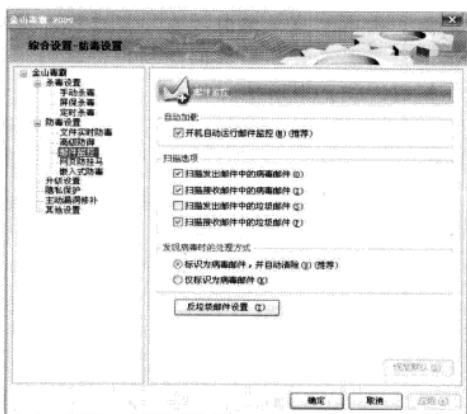
黑客攻防技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



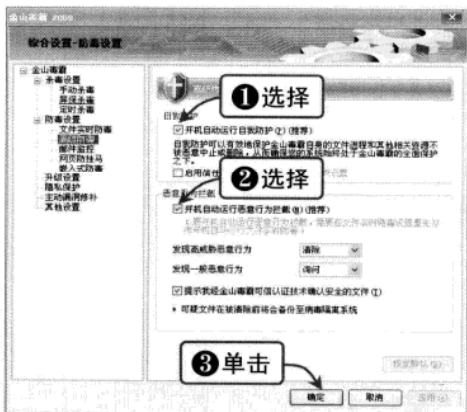
STEP 03 邮件监控

根据“邮件监控”对话框的各种设置，确保每一封发出和接收的邮件都受到监控保护，并对携带病毒邮件做出及时处理，如下图所示。



STEP 04 恶意行为拦截

选中“开机自动运行自我防护（推荐）”和“开机自动运行恶意行为拦截（推荐）”复选框，可有效地拦截电脑在开机和运行过程中出现的恶意行为威胁，单击“确定”按钮，如下图所示。



12.1.2 卡斯基的使用

卡斯基是卡斯基实验室研发推出的一款杀毒软件，它基于最新的技术为电脑提供反病毒保护。卡斯基当前最新版本为 2010，是新一代的数据安全产品，官方主页地址为 <http://www.kaspersky.com.cn>。

Work1 安装设置

从网站上找到卡斯基 Windows 系统环境下的安装文件，单击相应的下载超链接进行下载，文件下载完毕后，双击其安装程序图标，运行卡斯基安装程序进行安装。

STEP 01 安装向导

运行卡斯基安装文件，显示“安装向导”窗口，单击“下一步”按钮，如下图所示。

STEP 02 许可协议

弹出“最终用户授权许可协议”对话框，单击“我同意”按钮才能继续安装，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件



卡斯基反病毒软件 2010

欢迎使用卡斯基反病毒软件 2010 安装向导。

该安装向导将在您的计算机上安装卡斯基反病毒软件 2010 (9.0.0.736)。

在继续安装之前我们建议您关闭所有其它程序。

点击“下一步”继续安装。

点击“取消”退出安装向导。

如果您想在安装期间更改设置请选择“自定义安装”(建议高级用户使用)。

单击

☐ 自定义安装

下一步(N) > 取消(C)

STEP 03 加入卡斯基安全网络

在“卡斯基安全网络服务”对话框中，选中“我接受加入卡斯基安全网络条款”复选框，单击“安装”按钮，如下图所示。



卡斯基反病毒软件 2010

卡斯基安全网络服务

请阅读下列有关加入卡斯基安全网络的条款。

请阅读下面卡斯基安全网络数据收集声明，以决定您是否要加入卡斯基安全网络。

卡斯基安全网络数据收集声明

A. 简介

在您继续使用我们的服务或软件之前请仔细阅读该文档，其中包含您需了解的重要信息。如果您继续使用卡斯基实验室软件和服

务，您已同意卡斯基实验室数据收集声明，我们保留随时更改该声明的权利，并将更改公布在网页中。在

☒ 我接受加入卡斯基安全网络条款(A)

单击

< 上一步(B) 安装(I) 取消(C)

STEP 05 选择更新模式

在安装过程中软件会提示用户选择更新模式，选中“自动更新”单选按钮，单击“下一步”按钮继续安装，如下图所示。



卡斯基反病毒软件配置向导

更新

请选择更新模式。

请选择更新模式。

☒ 自动更新 (推荐) (A)

☐ 按计划更新(H)

☐ 手动更新(M)

设置(S)... 立即更新(U)

单击

< 上一步(B) 下一步(N) > 取消



卡斯基反病毒软件 2010

最终用户授权许可协议

请仔细阅读以下许可协议。

请阅读许可协议。您必须同意协议的所有条款才能安装。

卡斯基实验室最终用户许可协议

对所有用户的重要法律提示：在开始使用本软件之前请仔细阅读下列法律协议。

单击本许可协议窗口中的“我同意”按钮，表明您已经同意接受此协议的条款和条件的约束。这一举动等同于您的签名，表示您已同意接受此协议的约束并成为此协议中的一方，并承认本软件为专有软件，并禁止您向他人复制或分发。

单击

< 上一步(B) 我同意(A) 取消(C)

STEP 04 选择保护模式

在安装过程中，用户可以自行选择卡斯基的保护模式。推荐选择程序自动处理模式。选中自动处理复选框，单击“下一步”按钮，如下图所示。



卡斯基反病毒软件配置向导

保护模式

请选择保护模式。

您信任卡斯基反病毒软件并选择在发现计算机威胁时由该程序自动处理，不需要询问我 (推荐)

☒ 我选择自己处理计算机安全威胁，卡斯基反病毒软件处理安全威胁时每次都要询问我(我)

单击

< 上一步(B) 下一步(N) > 取消

STEP 06 完成程序安装

此时，卡斯基自动连接到官方服务器进行病毒库的升级，并完成软件的安装操作，如下图所示。



17% - 更新中心

正在更新 17%

运行时间: 00:00:38

更新大小: 1.9 MB

传输速率: 64 KB/秒

正在下载: index/.bases/av/ndb/386/basendic.kdc

位置: http://dl-12.geo.kaspersky.com/

帮助 取消

- 黑客
- 常用扫描
- 与嗅探工具
- 系统漏洞
- 安全策略
- 设置系统
- 系统安全
- 远程控制
- 木马
- 聊天软
- 网页恶
- 代码防
- 电子邮
- C盘病
- 使用电
- 黑客攻



Work2 保护中心

卡巴斯基的保护中心可以实时保护用户的电脑免受恶意程序和非法访问的威胁，同时还保障用户安全地访问网络。

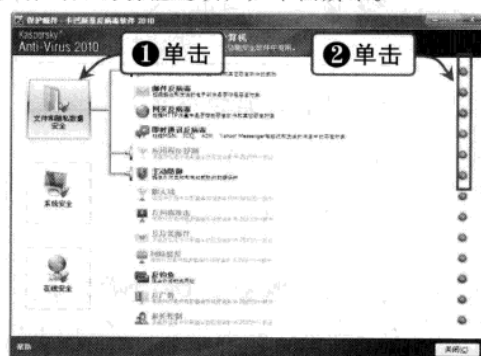
STEP 01 保护中心

卡巴斯基主界面的“保护中心”分为“文件和隐私数据安全”、“系统和应用程序安全”和“网络在线安全”三部分，如下图所示。



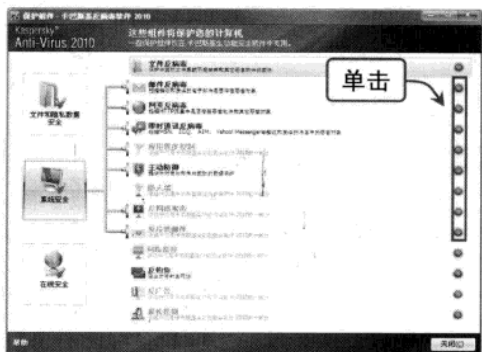
STEP 02 文件和隐私数据安全设置

单击“文件和隐私数据安全”选项，进入保护中心设置窗口。在“文件和隐私数据安全”选项中，单击右侧圆形按钮，可以打开或关闭具体对应的功能选项，如下图所示。



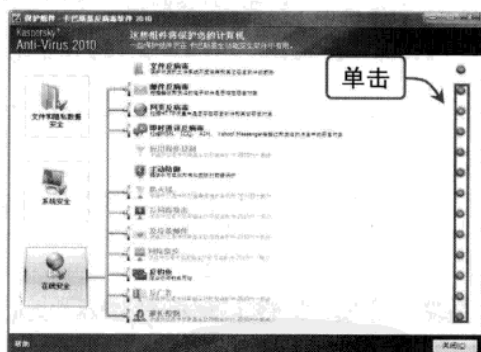
STEP 03 系统安全设置

在“系统安全”选项中，单击右侧圆形按钮，可以打开或关闭具体对应的功能选项，如下图所示。



STEP 04 在线安全设置

在“在线安全”选项中，单击右侧圆形按钮，可以打开或关闭具体对应的功能选项，如下图所示。



Work3 扫描中心

卡巴斯基另一项强大的功能是扫描，卡巴斯基的扫描中心可以扫描用户电脑中的病毒、木马、蠕虫、软件漏洞和其他威胁。

STEP 01 扫描中心

在卡巴斯基主界面中单击“扫描中心”按钮，显示扫描中心界面，如下图所示。

STEP 02 实施扫描

用户可以进行全盘扫描、快速扫描、对象扫描和漏洞扫描。单击“开始快速扫描”按钮，卡巴斯基会立即开始扫描所有操作系统启动时加载的对象，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件

单击

单击

Work4 软件设置

卡斯基可以由用户自己对各项功能进行设置，以达到更好的效果。单击卡斯基主界面右上角的“设置”按钮，进入“配置常规保护设置”界面。

STEP 01 配置常规保护设置

在“配置常规保护设置”窗口中，通过选中“启用保护”复选框，可以开启卡斯基的实时保护功能，单击“确定”按钮完成设置，如下图所示。

STEP 02 配置扫描任务设置

单击“扫描我的电脑”选项，显示“配置扫描任务常规设置”窗口，可以对扫描方式和扫描范围进行设置，单击“确定”按钮完成设置，如下图所示。

12.1.3 瑞星杀毒软件的使用

瑞星杀毒软件是一款优秀的国产杀毒软件，由北京瑞星科技股份有限公司开发，用于防止电脑遭受病毒入侵和有害程序破坏，有效维护电脑系统的安全。通过独创的三重病毒分析过滤技术，既能通过特征值查出已知病毒，又可以通过程序分析出未知的病毒，从而大大提高了预防病毒的能力。

Work1 瑞星的安装

用户可以从瑞星官方网站进行下载，下载后，运行安装程序进行如下安装。

STEP 01 语言选择

双击运行瑞星杀毒软件的安装程序，在显示的语言对话框中，可以选择“中文简体”、“中文繁体”和 English 三种语言中的一种，单击“确定”按钮开始安装，如下图所示。

STEP 02 最终用户许可协议

阅读《最终用户许可协议》，选中“我接受”单选按钮，单击“下一步”按钮继续，如下图所示。

基础入门

黑客知识

常用扫描

Windows 系统

设置系统

安全策略

系统与文

件加密

远程控

制攻防

木马

聊天软

件攻防

网页恶意

代码攻防

电子邮箱

件攻防

电子邮

件攻防

攻击防

毒攻防

安全软

件

使用电

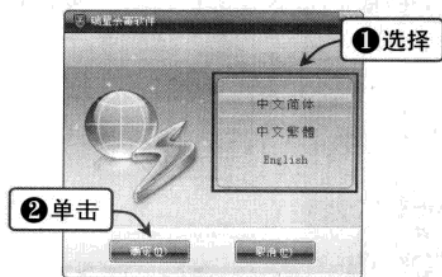
脑

黑客攻

防技巧

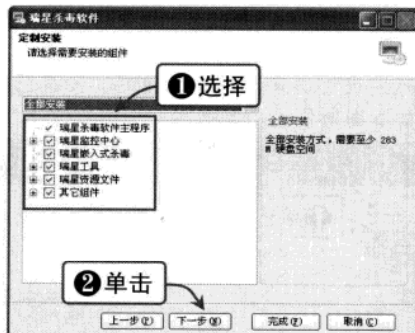
溜客安全网 WwW.176Ku.CoM

259



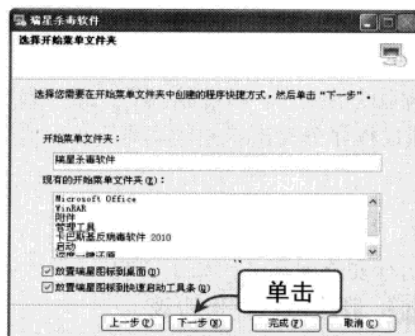
STEP 03 定制安装

在“定制安装”窗口中，可以在列表中选择需要安装的组件，单击“下一步”按钮继续安装，如下图所示。



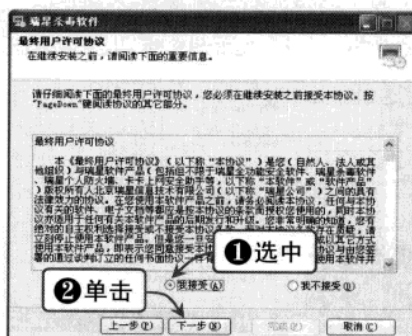
STEP 05 安装信息

在安装信息窗口中，显示了默认开始菜单文件夹，选择需要创建的快捷方式，单击“下一步”按钮，继续安装，如下图所示。



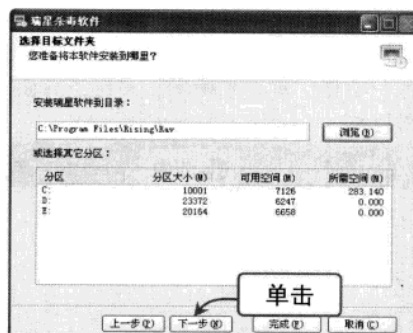
Work2 瑞星设置向导

瑞星设置向导会引导用户根据需要，提前对软件进行必要的设置。



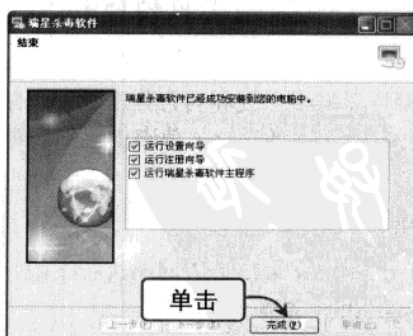
STEP 04 选择安装目录

在“选择目标文件夹”窗口中，用户可以指定瑞星杀毒软件的安装目录，单击“下一步”按钮继续安装，如下图所示。



STEP 06 完成程序安装

依次单击“下一步”按钮继续安装，当出现“结束”窗口时，单击“完成”按钮完成安装，如下图所示。

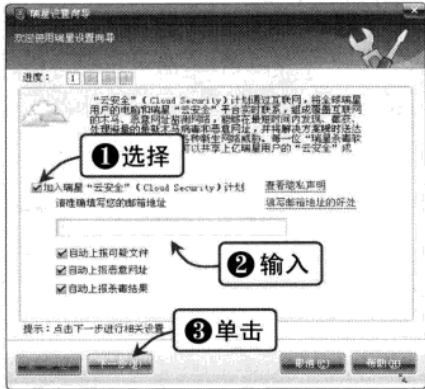


免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件

STEP 01 加入“云安全”计划

在瑞星设置向导中，选中“加入瑞星‘云安全’计划”复选框，并准确填写邮箱地址，即可加入瑞星的“云安全”计划，单击“下一步”按钮，如下图所示。



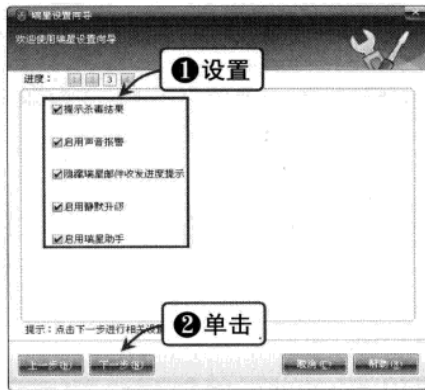
STEP 02 设置防御级别及处理方式

在“瑞星设置向导”对话框的“病毒处理设置”选项区中，可以设置病毒查杀、监控等各项功能的防御级别及处理方式，单击“下一步”按钮，如下图所示。



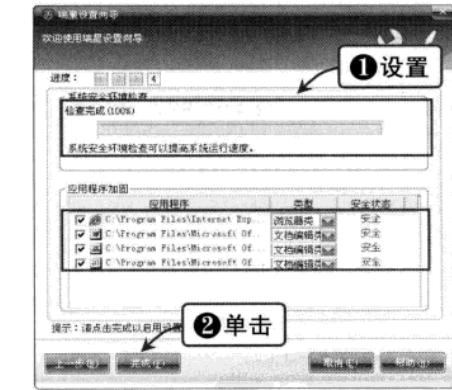
STEP 03 其他设置选项

用户可以通过选中“提示杀毒结果”、“启用声音报警”、“启用瑞星助手”等复选框进行设置，单击“下一步”按钮，如下图所示。



STEP 04 系统环境检查和文件加固

为了提高系统运行速度，用户可以在此进行系统安全环境检查，同时也可以对应用程序加固进行设置，单击“完成”按钮即可完成设置向导，如下图所示。



提示

瑞星“云安全”计划是指通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

Work3 手动杀毒

使用瑞星可以对用户指定的文件或文件夹进行手动杀毒，下面介绍手动杀毒的具体操作步骤。

基础知识

常用扫描与嗅探工具

系统漏洞攻防

安全策略

系统加密

远程攻击

木马

聊天软件

网页恶意代码

电子邮件

C盘病毒

使用安全软件

黑客攻防

黑客技巧



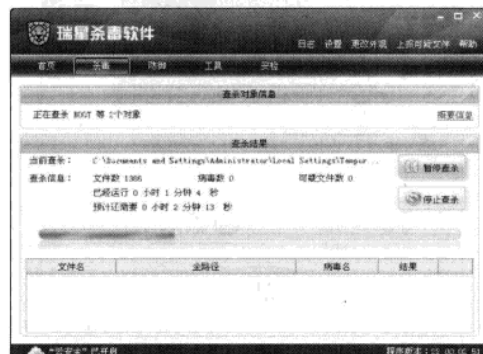
STEP 01 选择查杀目标

选择瑞星杀毒软件主界面的“杀毒”选项卡，依次展开“我的电脑\本地磁盘 (C:) \ WINDOWS”分支，选择要查杀的文件或文件夹，单击“开始查杀”按钮开始杀毒，如下图所示。



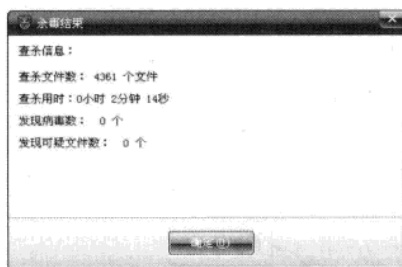
STEP 02 查杀过程

在查杀过程中，文件数、病毒数和查杀百分比将显示在查杀窗口下部。在扫描过程中，可以随时单击“暂停查杀”按钮来暂时停止查杀病毒，或单击“停止查杀”按钮停止查杀病毒，如下图所示。



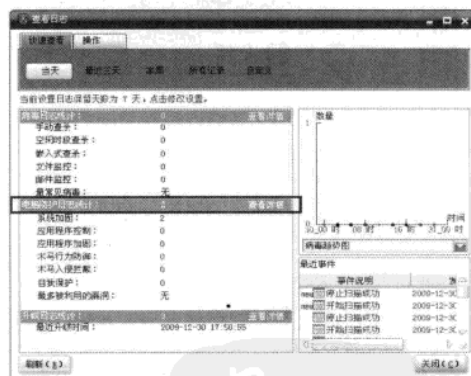
STEP 03 查杀结束

查杀结束后，将会显示查杀文件数、用时、发现病毒数以及发现可疑文件数等信息，如下图所示。



STEP 04 查看日志

查杀结束后，扫描结果将自动保存到杀毒软件工作目录的指定文件中，可以通过主界面中“日志”菜单项来查看以往的查杀病毒记录，如下图所示。



Work4 空闲时段杀毒

瑞星的定时杀毒功能能够自动完成病毒的查杀，不用人工干涉。下面将详细介绍进行定时杀毒的具体操作方法。

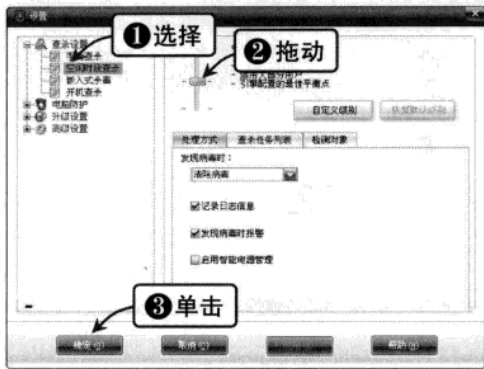
STEP 01 设置安全级别

在“设置”菜单项中选择“空闲时段查杀”选项，拖动滑块选择高、中、低三种查杀级别，单击“确定”按钮，如下图所示。

STEP 02 添加查杀任务

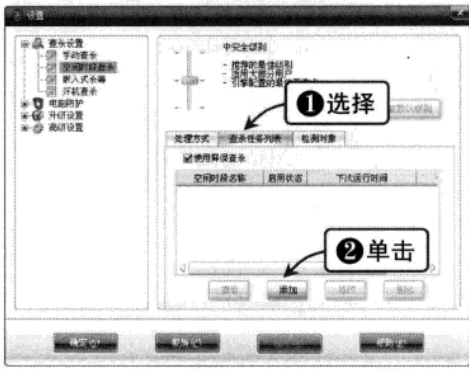
选择“查杀任务列表”选项卡，单击“添加”按钮，如下图所示。

Chapter 12 使用电脑安全软件



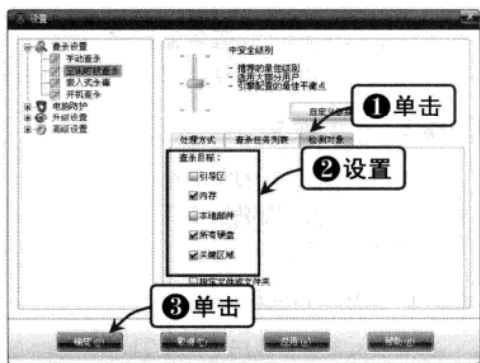
STEP 03 添加查杀时段

在“添加时段”对话框中，用户可以输入任务名称，描述、设置查杀类型及具体的开始/结束时间，单击“确定”按钮，如下图所示。



STEP 04 设置检测对象

选择“检测对象”选项卡，可以设置引导区、内存、本地邮件、所有硬盘、关键区或对指定文件或文件夹进行检测，单击“确定”按钮，如下图所示。



Work5 防御和监控

瑞星杀毒软件具有对病毒的智能主动防御和实时监控功能。智能主动防御是一种阻止恶意程序执行的技术，用户可以根据自己系统的特殊情况制定独特的防御规则，使主动防御可以最大限度地保护系统。实时监控用于实时地监控系统中的文件操作以及对接收和发送的邮件进行病毒扫描，防止病毒通过邮件传播感染电脑。

STEP 01 智能主动防御

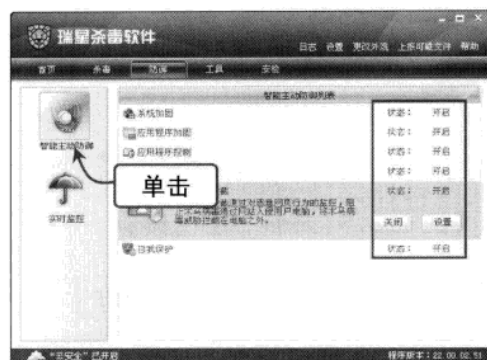
选择瑞星杀毒软件主界面的“防御”选项卡，单击“智能主动防御”按钮，单击“关闭”或“开启”按钮，可以对相关功能进行关闭和开启，如下图所示。

STEP 02 实时监控功能

选择瑞星杀毒软件主界面中的“防御”选项卡，单击“实时监控”按钮，单击“关闭”或“开启”按钮可以对相关功能进行关闭和开启，如下图所示。

基础
知识
与
嗅
探
工
具
常用扫描
Windows
统
漏
洞
攻
防
设置系统
安全策略
系统
与
文
件
加
密
远程
控
制
攻
防
木
马
聊天
软
件
攻
防
网
页
恶
意
代
码
攻
防
电
子
邮
件
攻
防
C
盘
病
毒
攻
防
黑
客
攻
防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



12.1.4 NOD32 的使用

NOD32 是斯洛伐克的 Eset 公司开发的杀毒软件。NOD32 支持 Windows、Linux、FreeBSD 以及其他系统平台。NOD32 非常轻巧易用。NOD32 的优点在于它的体积轻巧，占用资源小，具有惊人的侦测速度及卓越的性能。NOD32 在国际最权威的杀软评测 VB100%上一直保持通过率最高的记录。

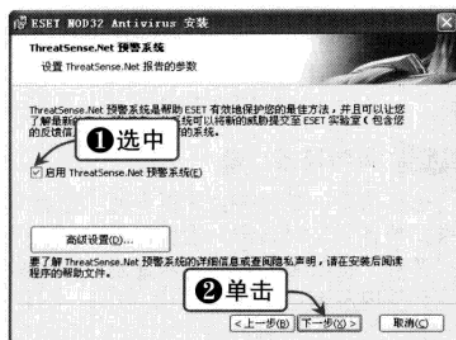
NOD32 在其高级启发式引擎中采用了云技术，称之为 ThreatSense.Net 预警系统。当杀毒引擎发现某个软件非常可疑，但又不足以认定它是病毒时，ThreatSense.Net 就会收集软件的相关信息，并与中心服务器交换资料，中心服务器通过所有收集到的资料便能够迅速、准确地做出反馈，即可侦测出最新的变种病毒，并成功阻挡病毒的散播。

Work1 安装设置

从 NOD32 官方网站 <http://www.eset.com.cn> 上找到 Windows 系统环境下的安装文件，单击相应的下载超链接进行下载。文件下载完毕后，双击其安装程序图标，运行 NOD32 安装程序，并进行安装。

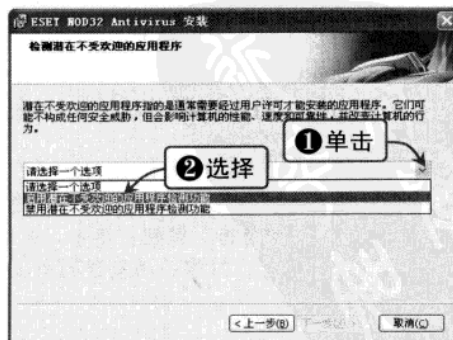
STEP 01 启用 ThreatSense.Net 预警系统

在安装过程中，选中“启用 ThreatSense.Net 预警系统”复选框，单击“下一步”按钮，如下图所示。



STEP 02 检测功能

在“检测潜在不受欢迎的应用程序”对话框中单击下拉按钮，在弹出的下拉列表中选择“启用潜在不受欢迎的应用程序检测功能”选项，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

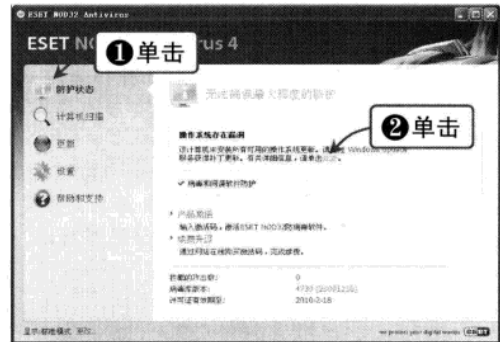
Chapter 12 使用电脑安全软件

Work2 安全防护

NOD32 运行时会自动检测系统漏洞，并提出检测结果报告。

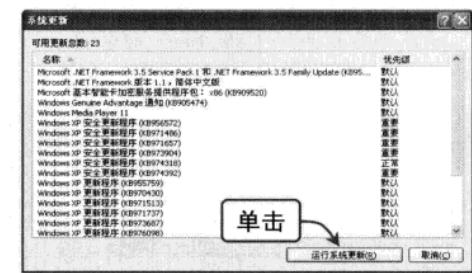
STEP 01 检测系统漏洞

在 NOD32 主界面中单击“防护状态”按钮，单击“此处”超链接，如下图所示。



STEP 02 查看需要更新的内容

“系统更新”对话框中以列表形式显示系统可用的更新详细内容。单击“运行系统更新”按钮，自动进行更新，如下图所示。

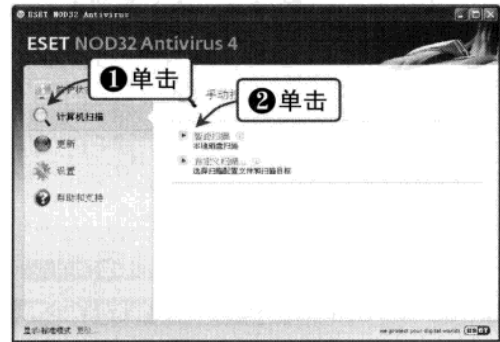


Work3 电脑扫描

NOD32 在系统后台自动进行扫描，如果用户怀疑自己的电脑已经感染病毒，则可以使用手动扫描的方式进行查杀。手动扫描分为智能扫描和自定义扫描两种。

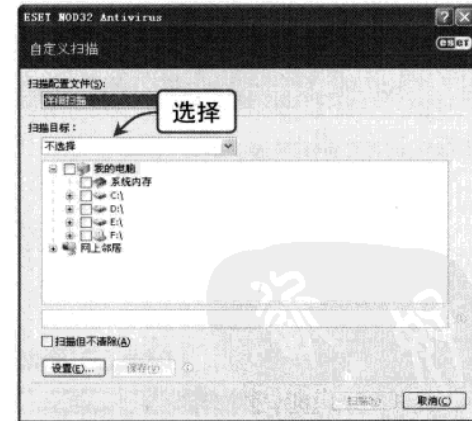
STEP 01 智能扫描

智能扫描也称标准扫描，使用默认设置扫描所有本地磁盘并且自动清除威胁。单击“计算机扫描”按钮，再单击“智能扫描”按钮，即可开始扫描，如下图所示。



STEP 02 自定义扫描

单击“计算机扫描”按钮，再单击“自定义扫描”按钮，弹出“自定义扫描”对话框，由用户自主选择扫描目标，如下图所示。



12.1.5 Norton AntiVirus 的使用

Norton AntiVirus 是一套强力的防毒软件，它会自动定期下载定义更新，每当开机时自动防护便会常驻在 System Tray，保护用户电脑免遭所有类型病毒和未知威胁的侵害。此外，

黑客
常用扫描
与嗅探工具
系统漏洞攻击
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
网页恶意
代码攻防
电子邮件
C 盘病毒
使用电脑
安全软件
黑客攻防
实用技巧



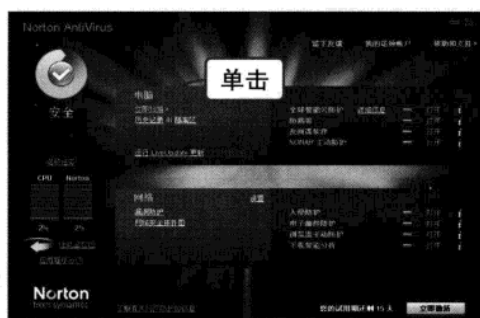
Norton AntiVirus 还会监控 Internet 活动，以帮助用户电脑抵御基于 Internet 且利用软件漏洞的威胁。

Work1 电脑扫描

如果用户怀疑电脑受到感染，则可以手动运行扫描功能进行病毒的查杀，具体操作步骤如下：

STEP 01 手动扫描

在 Norton AntiVirus 杀毒软件主界面的“电脑”选项卡中单击“立即扫描”超链接，如下图所示。

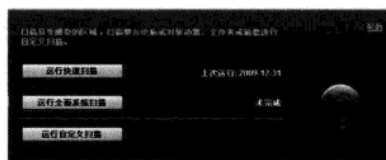


STEP 02 扫描类型

用户可单击按钮，选择下列三种扫描方式：
运行快速扫描：扫描病毒易攻击的目标电脑区域。

运行全面系统扫描：彻底检查用户电脑。

运行自定义扫描：扫描所有文件、文件夹、可移动驱动器或电脑的驱动器，如下图所示。



STEP 03 查看安全历史记录

在安全历史记录中，用户不但能看到扫描结果和已解决的安全风险，还能查看警报和事件消息的摘要。在 Norton AntiVirus 杀毒软件主界面的“电脑”选项卡中单击“历史记录”超链接，即可查看安全历史记录，如下图所示。



STEP 04 查看隔离区信息

Norton AntiVirus 对于实时监测到的安全风险和安全威胁一般放入隔离区，由用户决定要对这些项目采取何种操作。在 Norton AntiVirus 杀毒软件主界面的“电脑”选项卡中单击“隔离区”超链接，即可查看隔离区信息，如下图所示。



Work2 网络保护

网络防护可以扫描进出电脑的所有网络通信，并将此信息与一组攻击特征进行比较。攻击特征包含的信息可用于确定攻击者对已知操作系统或程序漏洞的利用企图，保护电脑不受最常见 Internet 攻击的侵害，主要有入侵防护、电子邮件防护和漏洞防护等。

Chapter 12 使用电脑安全软件

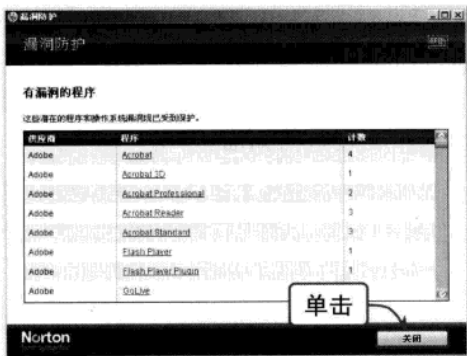
STTP 01 网络防护设置

在 Norton AntiVirus 杀毒软件主界面的“网络”选项卡中，单击“设置”超链接，打开“网络设置”窗口，可以通过拖动滑块开启或关闭各种防护设置，单击“确定”按钮，如下图所示。



STTP 02 查看漏洞防护

在 Norton AntiVirus 杀毒软件主界面的“网络”选项卡中单击“漏洞防护”超链接，将以列表形式显示用户电脑上的程序是否容易遭受恶意攻击的信息，并提供所抵御的已知攻击的信息，单击“关闭”按钮，如下图所示。



12.2 清理电脑中的恶意软件

恶意软件是指在未明确提示用户或未经用户许可的情况下，在用户电脑或其他终端上安装运行，侵害用户合法权益的软件，但不包含我国法律法规规定的电脑病毒。

12.2.1 恶意软件的特征

中国互联网协会反恶意软件协调工作组确定，具有下列特征之一的软件可以被认为是恶意软件：

- ❖ 强制安装：指未明确提示用户或未经用户许可，在用户电脑或其他终端上安装软件的行为。
- ❖ 难以卸载：指未提供通用的卸载方式，或在不受其他软件影响、人为破坏的情况下，卸载后仍然有活动程序的行为。
- ❖ 浏览器劫持：指未经用户许可，修改用户浏览器或其他相关设置，迫使用户访问特定网站或导致用户无法正常上网的行为。
- ❖ 广告弹出：指未明确提示用户或未经用户许可，利用安装在用户电脑或其他终端上的软件弹出广告的行为。
- ❖ 恶意收集用户信息：指未明确提示用户或未经用户许可，恶意收集用户信息的行为。
- ❖ 恶意卸载：指未明确提示用户、未经用户许可，或误导、欺骗用户卸载其他软件的行为。
- ❖ 恶意捆绑：指在软件中捆绑已被认定为恶意软件的行为。
- ❖ 其他侵害用户软件安装、使用和卸载知情权、选择权的恶意行为。



12.2.2 常用恶意软件清理工具

用户无意中安装了恶意软件后，很难通过常规软件卸载方法进行清除，这时就需要使用专门的恶意软件清理工具进行清理。

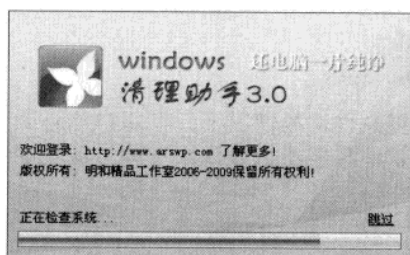
Work1 Windows 清理助手

Windows 清理助手能对已知的木马和恶意软件进行彻底的扫描与清理，提供系统扫描与清理和在线升级功能，独特的清理方式使清理助手能轻易对付强行驻留系统、变名等一系列恶意行为的软件。Windows 清理助手是免费软件，电脑用户可以从 <http://www.arswp.com/download.html> 进行下载。

Windows 清理助手的具体使用方法如下：

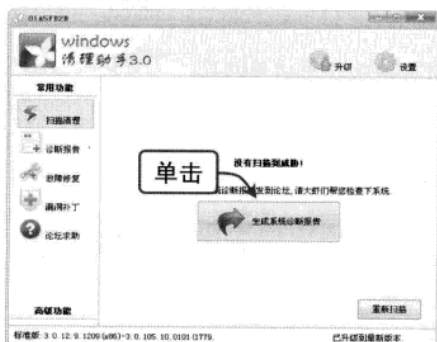
STEP 01 自动进行扫描

Windows 清理助手运行时，首先会对系统自动进行扫描，并显示扫描的进度，其界面如下图所示。



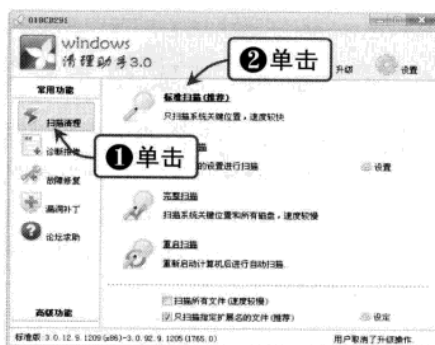
STEP 03 生成系统诊断报告

系统扫描完成后，打开“扫描完成”窗口，单击“生成系统诊断报告”按钮，Windows 清理助手会生成一份针对用户电脑的系统诊断报告，用户可以把生成的报告发到网络上以寻求帮助，如下图所示。



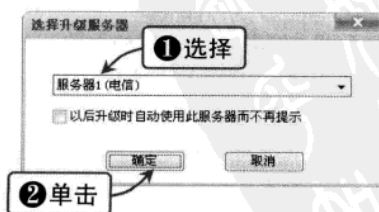
STEP 02 标准扫描

在 Windows 清理助手主界面中单击“扫描清理”按钮，再单击“标准扫描（推荐）”按钮，开始系统扫描，如下图所示。



STEP 04 自动网络升级

在 Windows 清理助手主界面中单击右上角“升级”按钮，弹出“选择升级服务器”对话框，在下列表框中选择合适的服务器，单击“确定”按钮，Windows 清理助手即可自动进行网络升级，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件

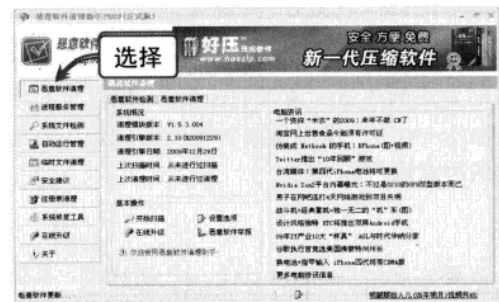
Work2 恶意软件清理助手

恶意软件清理助手是 Tomm 软件工作室开发的一款免费的恶意软件清理软件，电脑用户可以从 <http://www.tommsoft.com/Products.aspx> 进行下载。

恶意软件清理助手的具体使用方法如下：

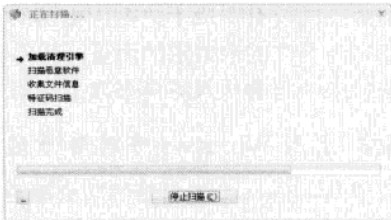
STEP 01 选择“恶意软件检测”选项卡

运行恶意软件清理助手，单击“恶意软件清理”按钮，选择“恶意软件检测”选项卡，如下图所示。



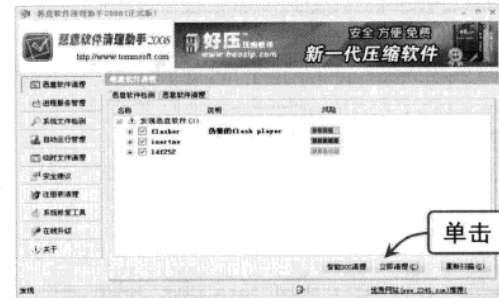
STEP 02 开始扫描

单击“基本操作”选项区中的“开始扫描”选项，软件将弹出“正在扫描”对话框，实时显示扫描过程，直至扫描结束，如下图所示。



STEP 03 扫描结果

扫描结果显示在“恶意软件清理”选项卡中，单击“立即清理”按钮，如下图所示。



STEP 04 清理结果

清理完成后，显示清理结果，如下图所示。



12.3 使用防火墙抵御网络攻击

随着网络技术的迅猛发展，网络安全的问题已经日益突出地摆在各类用户面前。目前，在互联网上大约有将近 20% 以上的用户曾经遭受过黑客的困扰。目前存在这样一个事实，大多数的黑客入侵事件都是由于未能正确安装防火墙而引发的。只有电脑用户正确地安装使用防火墙，才能对网络攻击实施有效的防护。

12.3.1 Windows 系统自带的防火墙

Windows 操作系统中自己带有网络防火墙，极大地方便了一般电脑用户的使用。下面将

黑客
常用扫描
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
网页恶意
代码攻防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客攻防
实用技巧



以 Windows XP 系统自带防火墙为例进行介绍。



提示

防火墙的本义指古代人们房屋之间修建的那道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋。而这里所说的防火墙是指隔离在本地网络与外界网络之间的一道防御系统，有以软件形式运行在普通电脑之上的，也有以固件形式设计在路由器之中的。防火墙是这一类防范措施的总称。

Work1 Windows 系统自带的防火墙简介

Windows 系统自带的防火墙是一个基于主机的状态防火墙，它丢弃所有未请求的传入流量，即那些既没有对应于为响应电脑的某个请求而发送的流量（请求的流量），也没有对应于已指定为允许的未请求的流量（异常流量）。Windows 防火墙提供某种程度的保护，避免那些依赖未请求的传入流量来攻击网络上的电脑的恶意用户和程序。

Work2 启用 Windows 系统自带的防火墙

要使 Windows 系统自带的防火墙正常工作，就要先启用 Windows XP 中的防火墙，具体操作步骤如下：

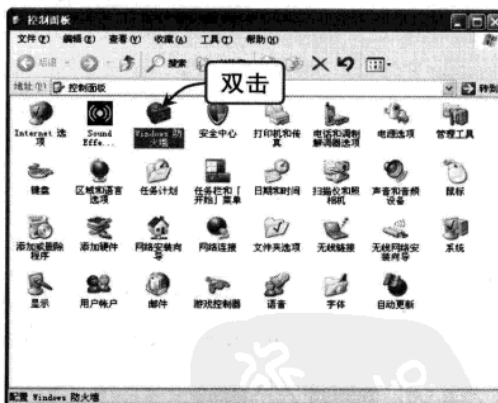
STEP 01 打开控制面板

单击“开始”|“控制面板”命令（如下图所示），打开“控制面板”窗口。



STEP 02 打开 Windows 防火墙设置

在“控制面板”窗口中双击“Windows 防火墙”图标，打开 Windows 防火墙设置，如下图所示。



STEP 03 启用防火墙

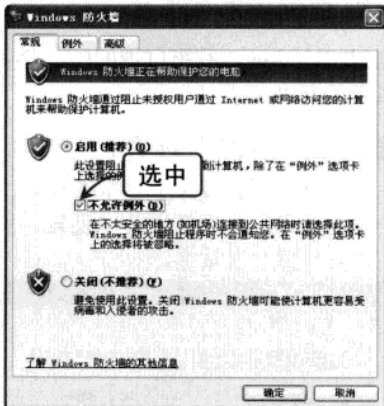
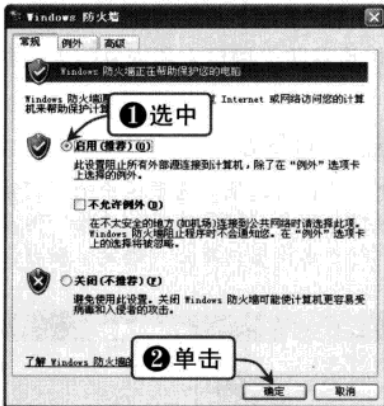
弹出“Windows 防火墙”对话框，在“常规”选项卡中选中“启用（推荐）”单选按钮，单击“确定”按钮，启用 Windows 系统自带的防火墙，如下图所示。

STEP 04 “不允许例外”选项

“不允许例外”选项比较适用于连接在公共网络上个人电脑，它拦截了绝大部分应用程序，但仍然可以浏览网页、发送接收电子邮件，或者使用即时通信软件。在此选中“不允许例外”复选框，如下图所示。

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件



Work3 设置例外程序

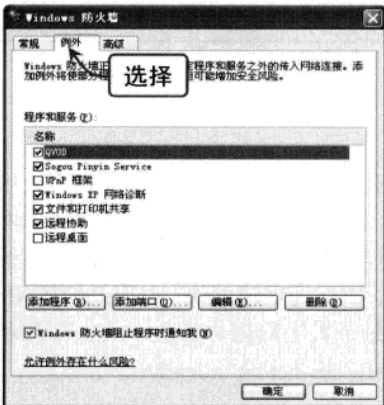
用户允许的程序和服务可以在 Windows 系统自带的防火墙中设置为例外程序，具体操作方法如下：

STEP 01 选择“例外”选项卡

在“常规”选项卡中取消选择“不允许例外”复选框，选择“例外”选项卡，在“程序和服务”列表中会显示通过 Windows 防火墙的程序和服务，选中复选框的表示允许通过防火墙，如下图所示。

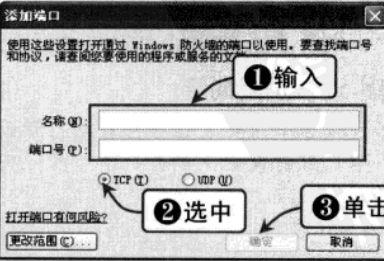
STEP 02 添加程序

单击“添加程序”按钮，添加允许通过防火墙的程序。在“添加程序”对话框的“程序”列表框中选择要添加的程序，单击“确定”按钮，如下图所示。



STEP 03 添加端口

单击“添加端口”按钮，弹出“添加端口”对话框。选择要添加的端口，可以更改应用程序的允许访问端口，输入名称后在端口号中输入允许的端口号，然后选中 TCP 或者 UDP 网络协议，单击“确定”按钮，如右图所示。



黑客
基础入门
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客攻防
实用技巧

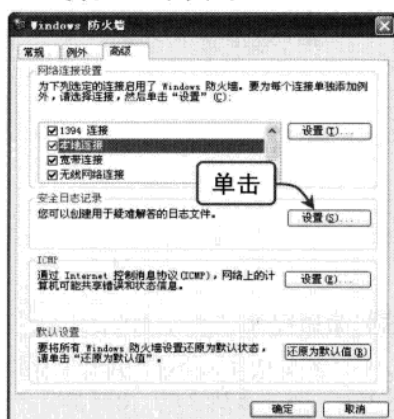


Work4 防火墙高级设置

通过 Windows 系统自带的防火墙高级设置，可以设置防火墙日志和恢复防火墙默认设置，具体操作步骤如下：

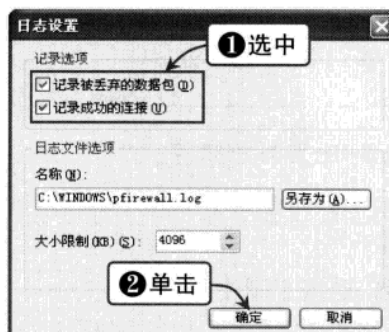
STEP 01 选择“高级”选项卡

选择“高级”选项卡，如下图所示。单击“安全日志记录”选项区中的“设置”按钮，弹出“日志设置”对话框。



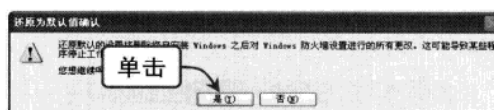
STEP 02 设置日志

选中“记录选项”选项区中的“记录被丢弃的数据包”和“记录成功的连接”两个复选框，进行日志设置，单击“确定”按钮，如下图所示。



STEP 03 恢复默认设置

单击“默认设置”选项区中的“还原为默认值”按钮，单击“确定”按钮，弹出如右图所示的提示信息框，单击“是”按钮。



12.3.2 “天网”个人防火墙

“天网”个人防火墙是由广州众达天网技术有限公司开发的国内第一款针对个人用户的软件防火墙，拥有强大的访问控制、信息过滤和自定义规则设置等功能，针对不同的网络环境灵活选择适当的安全方案，可以有效抵御木马、后门病毒、黑客攻击以及 IE、系统漏洞等安全隐患带来的威胁。最新版本的包过滤引擎内核，数据处理速度快，占用系统资源极低，能在正常上网的同时最大限度地保障您机器的安全，是个人上网用户防止个人文件和私密信息泄露的必备安全软件。用户可以到官方网站 <http://pfw.sky.net.cn/index.html> 下载。

Work1 安装设置

“天网”个人防火墙在安装过程中可以进行简单初始设置，具体操作步骤如下：

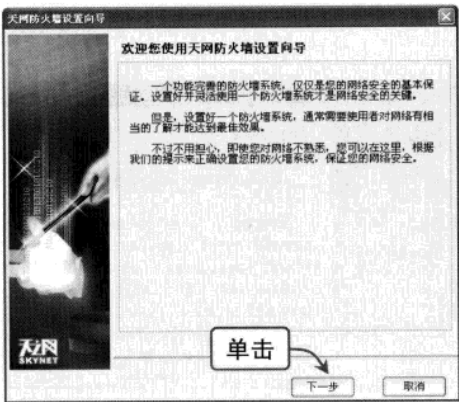
STEP 01 进入设置向导

安装过程中，安装程序会自动打开设置向导提示用户进行设置，单击“下一步”按钮，如下图所示。

STEP 02 安全级别设置

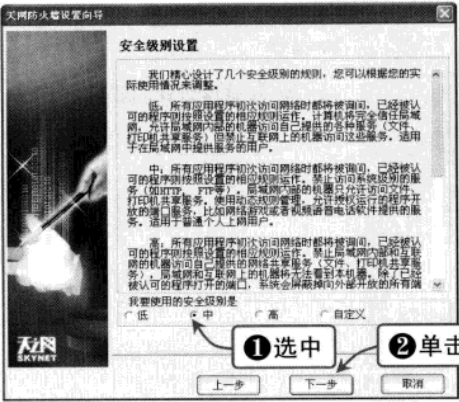
在“我要使用的安全级别是”选项区中，可以按用户需要选中“低”、“中”、“高”或“自定义”单选按钮。建议直接选中默认的“中”单选按钮，单击“下一步”按钮，如下图所示。

Chapter 12 使用电脑安全软件



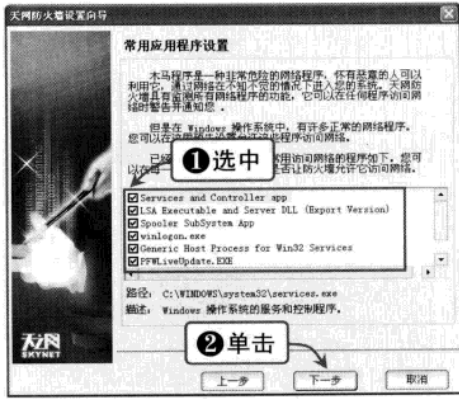
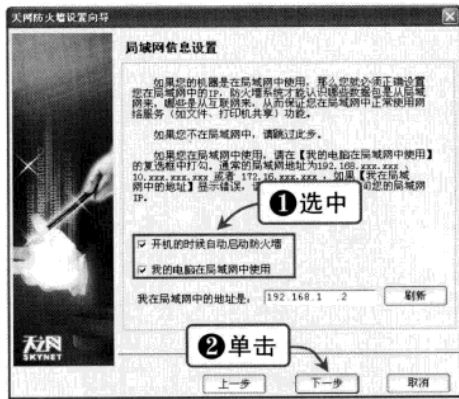
STEP 03 局域网设置信息

如果用户的电脑是在局域网中使用，就要选中“我的电脑在局域网中使用”复选框。选中“开机的时候自动启动防火墙”复选框，可以设置“天网”个人防火墙在用户电脑每次开机时自动在系统后台运行，单击“下一步”按钮，如下图所示。



STEP 04 应用程序设置

用户电脑系统中有正常的网络程序访问网络，也可能隐藏了木马程序偷偷访问网络，可以通过“常用应用程序设置”来预先设置允许正常的常用网络程序访问网络，从而禁止非法程序访问网络，达到保护用户电脑的目的。在列表框中选中所要允许的程序前的复选框，单击“下一步”按钮，如下图所示。



提示



在“常用应用程序设置”对话框中，用户可以对已知的正常的程序进行允许设置，这样在以后操作中就不用再对正常的程序一一进行设置了。

STEP 05 完成设置

在向向导设置完成界面单击“结束”按钮完成设置，如下图所示。

STEP 06 完成安装

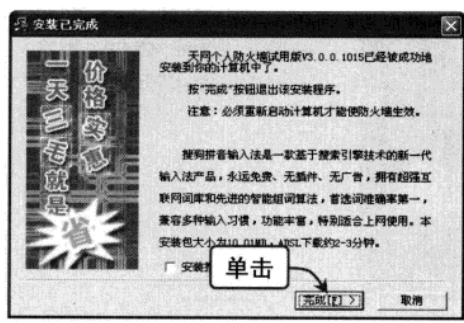
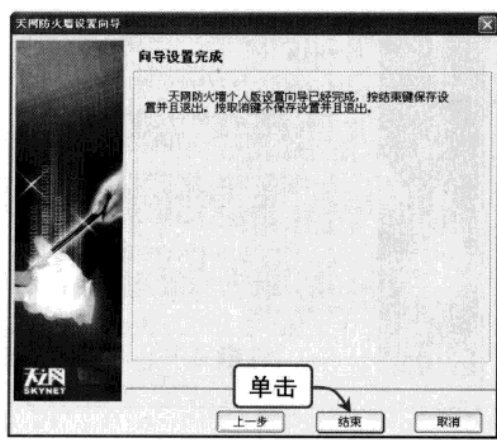
单击“完成”按钮，完成“天网”个人防火墙的安装过程，如下图所示。

黑客
基础
知识
与
嗅
探
工
具
统
漏
洞
攻
防
安全策略
设置系统
系统与安全
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防电子邮
件攻防
病毒防
使用电脑
安全软件
黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



黑客攻防从新手到高手

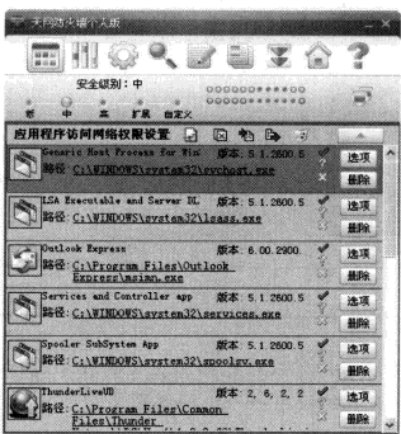


Work2 应用程序管理

“天网”个人防火墙可以对应用程序进行管理，详细设置其是否可以连接网络。下面以对系统自带的 IE 浏览器为例进行介绍，具体操作步骤如下：

STEP 01 程序访问网络权限设置

单击“天网”个人防火墙主界面中的“应用程序规则”按钮，打开“应用程序访问网络权限设置”对话框，在程序列表框中默认是没有 IE 浏览器的，如下图所示。

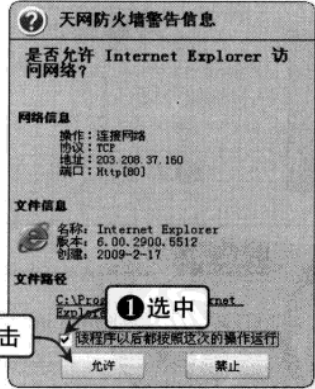


STEP 03 添加完成

此时程序列表中就有 IE 浏览器了，单击 IE 浏览器的路径超链接，显示 IE 浏览器执行文件的真实地址，如下图所示。

STEP 02 添加程序

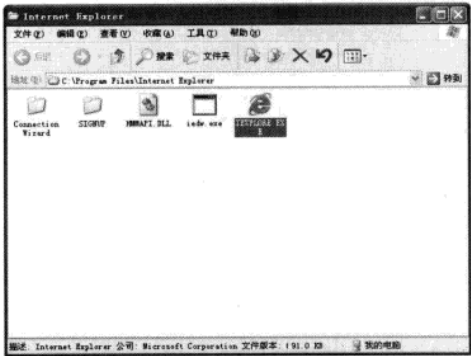
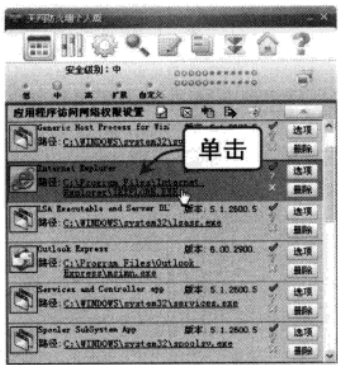
运行 IE 浏览器，打开任一网页，此时“天网”个人防火墙自动弹出“天网防火墙警告信息”对话框。显示 IE 浏览器相关的“网络信息”、“文件信息”和“文件路径”，并提示用户选择“允许”或“禁止”IE 浏览器访问网络，选中“该程序以后都按照这次的操作运行”复选框，单击“允许”按钮，如下图所示。



STEP 04 确定位置

系统自动打开显示 IE 浏览器真实位置的窗口。用户可以进一步进行核实，以确保程序真实有效，如下图所示。

Chapter 12 使用电脑安全软件

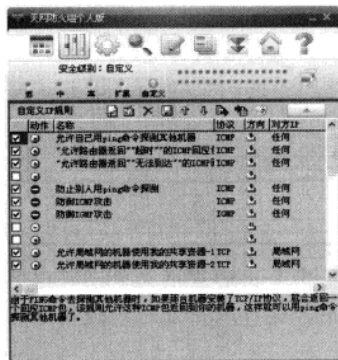


Work3 IP 规则管理

使用“天网”个人防火墙还可以进行详细的 IP 规则设置，具体操作步骤如下：

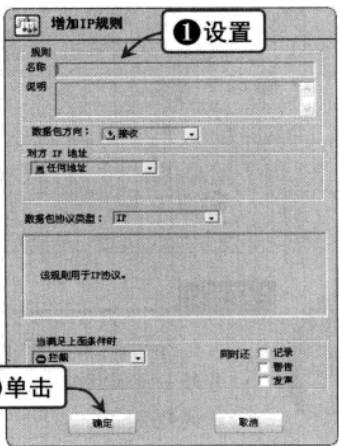
STEP 01 IP 规则管理

“天网”个人防火墙本身已经默认设置了相当好的缺省规则，一般用户并不需要做任何 IP 规则修改，可直接使用。单击主界面中的“IP 规则管理”按钮，弹出“自定义 IP 规则”对话框，在列表框中列出了默认的 IP 规则，单击每个规则，窗口会实时显示详细解释，如下图所示。



STEP 02 增加 IP 规则

在“自定义 IP 规则”窗口单击“增加规则”按钮，弹出“增加 IP 规则”对话框。可以增加新的 IP 规则，设置名称、规则等内容，单击“确定”按钮，如下图所示。



提示

IP 规则设置是“天网”个人防火墙软件中特有的功能，这项功能为用户提供了最大的自由，用户可以根据各自不同的情况来设置不同的 IP 规则。

STEP 03 修改规则

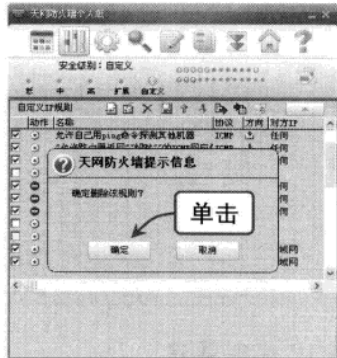
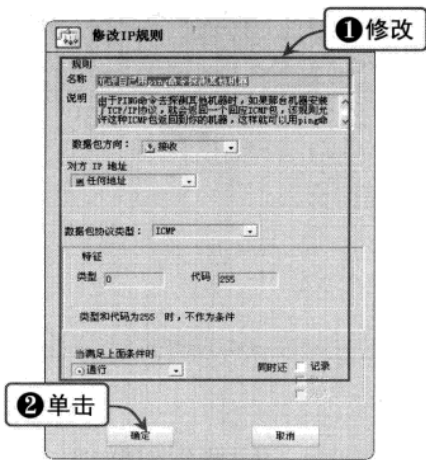
在“自定义 IP 规则”对话框列表选中要修改的 IP 规则，单击“修改规则”按钮，弹出“修改 IP 规则”对话框，可以修改 IP 规则的各项内容，单击“确定”按钮，如下图所示。

STEP 04 删除规则

在“自定义 IP 规则”对话框列表选中要删除的 IP 规则，单击“删除规则”按钮，系统提示删除确认信息，单击“确定”按钮，如下图所示。

黑客
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



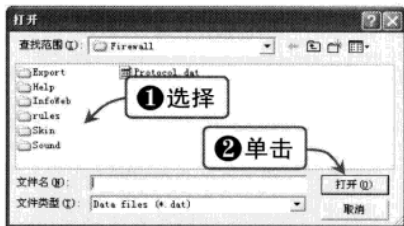
STEP 05 导出规则

单击“导出规则”按钮，单击“浏览”按钮选择规则文件的保存位置，并在规则列表中选导出规则前的复选框，单击“确定”按钮完成规则的导出，如下图所示。



STEP 06 导入规则

单击“导入规则”按钮，弹出“打开”对话框，选择要导入的规则文件，单击“打开”按钮，完成规则的导入，如下图所示。



提示

从一台电脑安装的天网防火墙软件中导出的规则文件，可以导入到另外一台电脑安装的天网防火墙软件中，这样用户就可以使用别人设置好的规则了。

Work4 软件设置

“天网”个人防火墙软件提供了详细的设置选项，可以对一些功能进行设置，具体操作步骤如下：

STEP 01 设置防火墙自动运行

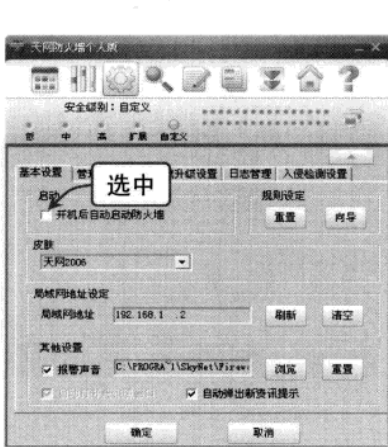
单击主界面中的“系统设置”按钮，选择“基本设置”选项卡，选中“开机后自动启动防火墙”复选框，如下图所示。

STEP 02 权限设置

选择“管理权限设置”选项卡，单击“设置密码”按钮，弹出“天网防火墙个人版密码保护”对话框，两次输入密码后，单击“确定”按钮。再单击“确定”按钮，完成设置，如下图所示。

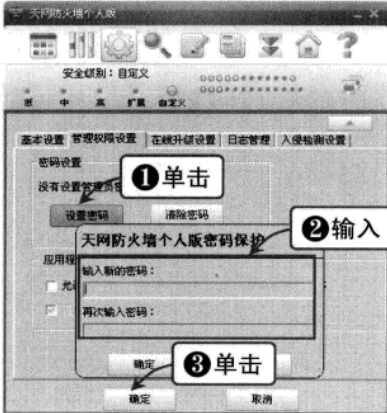
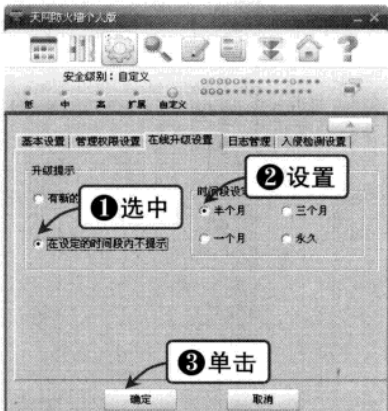
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件



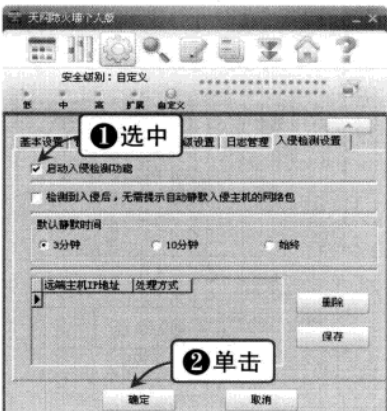
STEP 03 升级设置

选择“在线升级设置”选项卡，在“升级提示”选项区中选中“在设定的时间段内不提示”单选按钮，显示“时间段设定”选项区，可以设置“半个月”、“一个月”、“三个月”或“永久”，单击“确定”按钮，如下图所示。



STEP 04 启用入侵检测

选择“入侵检测设置”选项卡，选中“启动入侵检测功能”复选框，单击“确定”按钮，如下图所示。



Work5 查看实时网络状态

通过“天网”个人防火墙可以查看网络的实时状态，具体操作步骤如下：

STEP 01 选择网络协议

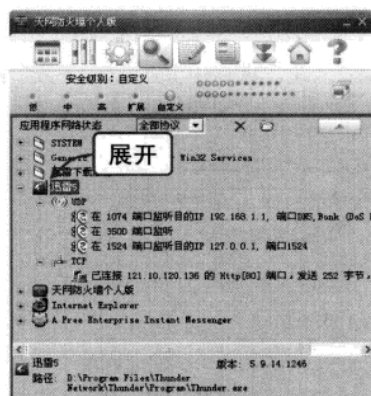
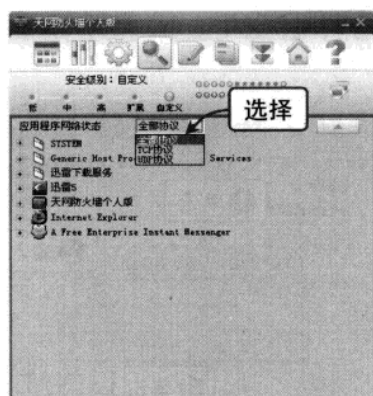
单击主界面中的“当前系统中所有应用程序网络使用状况”按钮，弹出“应用程序网络状态”对话框。单击下拉按钮，在弹出的下列列表中选择“全部协议”选项，如下图所示。

STEP 02 查看软件实时网络状态

展开程序列表中的“迅雷 5”分支，查看其下的 UDP 和 TCP 网络协议状态，如下图所示。

黑客
常用扫描
漏洞探测工具
系统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控制
木马
聊天软
网页恶意
代码攻防
电子邮箱
C盘病毒
使用电脑
安全软件
黑客攻防
实用技巧

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

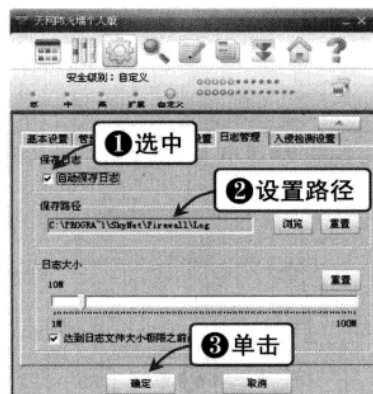


Work6 网络日志

“天网”个人防火墙的网络日志功能也非常强大，查看日志的具体操作步骤如下：

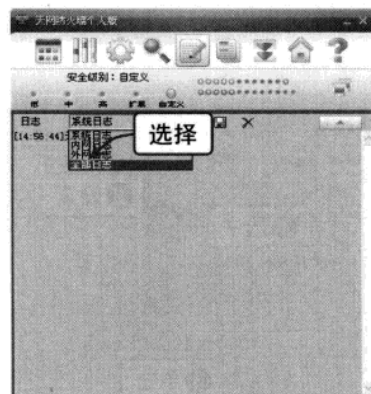
STEP 01 保存日志设置

单击主界面中的“系统设置”按钮，选择“日志管理”选项卡，选中“自动保存日志”复选框，单击“浏览”按钮可以设置日志保存的路径，单击“确定”按钮，如下图所示。



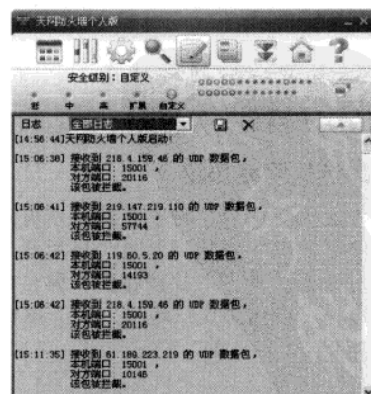
STEP 02 选择日志类别

单击主界面中的“日志”按钮，弹出“日志”对话框。单击下拉按钮，在弹出的下拉列表中选择“全部日志”选项，如下图所示。



STEP 03 查看日志

实时查看系统网络的全部日志，如右图所示。



提示

日志功能对一个合格的黑客来讲十分重要，通过日志可以对电脑的安全问题有一个详细的判断。

12.3.3 ZoneAlarm 个人网络防火墙

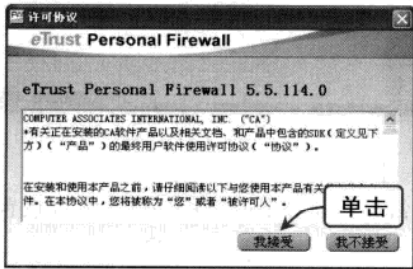
ZoneAlarm 是 Zone Labs 公司推出的一款防火墙软件。ZoneAlarm 使用很简单，用户安装完后重新开机，ZoneAlarm 就会自动启动，自动执行任务。用户可以自由设置所有程序是否允许连接 Internet，利用此种方法来防止一些来路不明的软件偷偷上网。最好的方法是锁住（Lock）网络不让任何程序通过，只有用户核准的软件才可以通行无阻。下面将以 ZoneAlarm Pro 5.5 官方中文版为例进行介绍。

Work1 软件安装

ZoneAlarm 的安装方法和一般 Windows 环境下的软件基本一致，安装完成后要重新启动电脑，软件才能运行。主要安装过程如下：

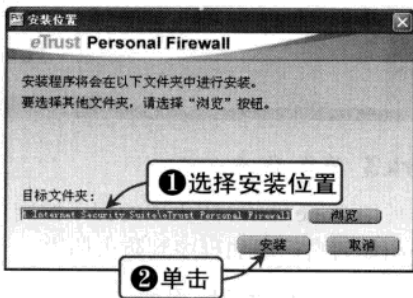
STEP 01 同意许可协议

运行 ZoneAlarm 的安装文件，弹出许可协议对话框，单击“我接受”按钮，继续安装，如下图所示。



STEP 02 设置安装位置

在“安装位置”对话框中单击“浏览”按钮，选择具体安装位置，单击“安装”按钮，开始程序的安装，如下图所示。

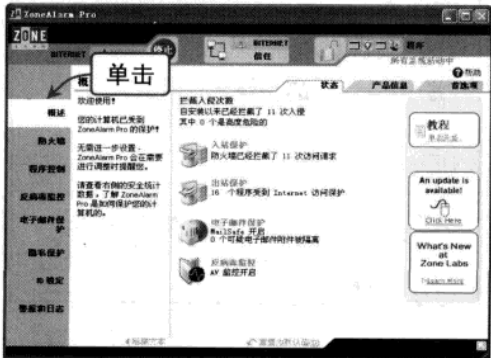


Work2 功能概述

ZoneAlarm 防火墙最大的特点是使用简单、功能强大，其基本功能有以下几种：

STEP 01 查看安全统计数据

在 ZoneAlarm 软件主界面中单击“概述”按钮，显示当前电脑的安装统计数据，如下图所示。



STEP 02 切断网络访问

在 ZoneAlarm 软件主界面中单击红色的“停止”按钮，可以立即关闭电脑与网络的连接，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

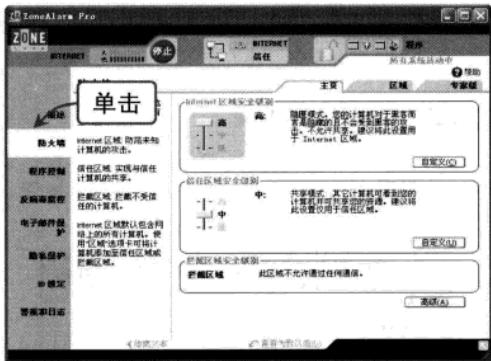


STEP 03 防火墙设置

防火墙功能可保护用户免受危险通信量的攻击，有三个区域：

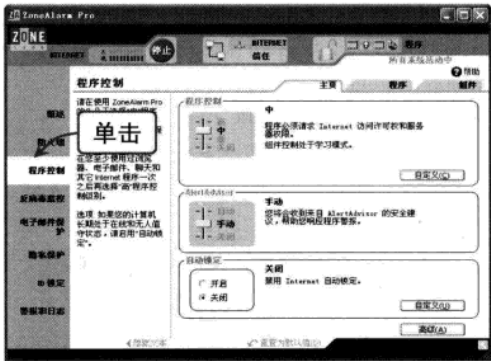
- Internet 区域：防范未知电脑的攻击。
- 信任区域：实现与信任电脑的共享。
- 拦截区域：拦截不受信任的电脑。

用户可以根据需要分别对三个区域进行级别设置。在 ZoneAlarm 软件主界面中单击“防火墙”选项，如下图所示。



STEP 04 程序设置

在 ZoneAlarm 软件主界面中单击“程序控制”按钮，用户可以在“程序控制”选项区中进行级别设置，如下图所示。



Work3 添加程序

使用 ZoneAlarm 防火墙的程序控制功能可以非常灵活地对上网的程序进行权限设置，下面介绍如何自己添加程序到防火墙中。

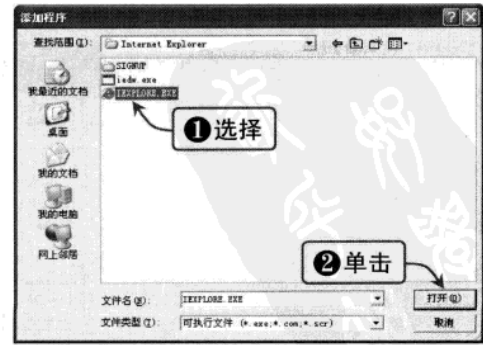
STEP 01 打开程序控制界面

在 ZoneAlarm 软件主界面中单击“程序控制”按钮。选择“程序”选项卡，当前系统中运行的程序就会以列表的形式显示在窗口中。有小绿点的表示此程序正在连接网络，如下图所示。



STEP 02 确定程序

单击上图中的“添加”按钮，弹出“添加程序”对话框。在“查找范围”下拉列表框中确定所要添加的程序，单击“打开”按钮，即可完成程序的添加，如下图所示。



免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12 使用电脑安全软件

STEP 03 添加完成

此时，添加的程序会出现在程序列表中，如右图所示。



提示

用户可以对添加的程序进行具体的信任设置，可以设置其网络及邮件的访问限制。



Work4 实时监控

ZoneAlarm 防火墙的监控功能分为对程序的监控和对网络的监控，下面进行简要介绍。

STEP 01 程序监控

如果有新的程序试图连接网络, ZoneAlarm 防火墙会在第一时间提出警告。下图所示为打开为 IE 浏览器时防火墙所提示的对话框。选中“记住此设置”复选框, 单击“允许”按钮。IE 浏览器就会加入到防火墙的信任程序列表中。



STEP 02 网络监控

如果有别的电脑对用户电脑进行扫描或攻击, ZoneAlarm 防火墙会弹出警告信息框, 如下图所示。用户可以根据不同情况采取相应的措施。



黑客
基础知识

Windows系统漏洞攻防

设置系统安全策略

系统与文
件加密

远程控
制攻防

防 马
聊天软件攻防

网页恶意
代码攻防

电子邮
件攻防
毒 口

以防 使用
安全

黑客工具
实用技术

OG

Chapter

13

黑客攻防实用技巧

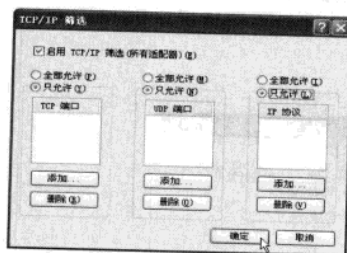
本章将汇总一些在实际应用过程中比较有实用价值的黑客攻防技巧，其中包括系统设置与账户管理技巧、系统应用与故障排除技巧、IE 浏览器安全应用技巧、常见病毒与木马的防范技巧等，读者应该熟练掌握并运用，以保证安全地使用电脑。

本章建议学习时间：

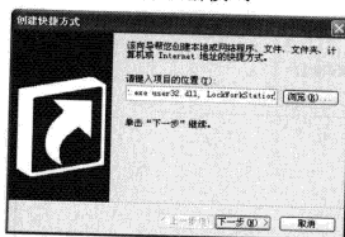
本章建议学习时间为 80 分钟，其中分配 50 分钟学习黑客攻防实用技巧的相关知识，30 分钟观看教学课件视频并进行练习。

学完本章后您可以：

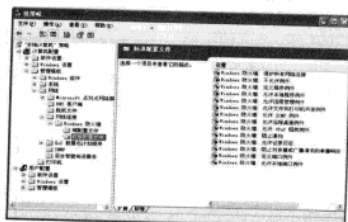
- 掌握系统设置与账户管理技巧
- 掌握系统应用与故障排除技巧
- 掌握 IE 浏览器常见应用技巧
- 掌握病毒和木马的防范技巧



选择更新模式



启动创建快捷方式向导



打开“组策略”窗口向导

重要知识点视频索引



13.1 系统设置与账户管理技巧

在黑客攻防方面，尤其要注意对系统设置与账户管理，只有为系统布置好“铜墙铁壁”，才能有效地防止黑客入侵。

13.1.1 Windows XP 中常见的系统进程

Windows XP 中常见的系统进程包括以下几个：

smss.exe：会话管理子系统，它负责启动用户会话。这个进程是通过系统进程来初始化的，包括对正在运行的 winlogon、Win32 (csrss.exe) 线程和设定的系统变量作出反映。在它启动这些进程后，它等待 winlogon 或者 csrss 结束。如果这些进程发生了什么不可预料的事情，smss.exe 就会让系统停止响应（就是挂起）。

csrss.exe：子系统服务器进程，这个用户模式 Win32 子系统的一部分。csrss 是一个基本的子系统，它必须一直运行。csrss 负责控制 Windows 创建或者删除线程。

winlogon.exe：管理用户登录程序。

services.exe：包含很多系统服务。

lsass.exe：管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序，会产生会话密钥以及授予用于交互式客户/服务器验证的服务凭据 (ticket)，也就是本地安全权限服务，属于 Windows 的核心进程之一，有名的震荡波病毒就是利用它的一个漏洞。

svchost.exe：svchost.exe 是从动态链接库 (DLL) 中运行的服务的通用主机进程名称，它是系统的核心进程。svchost.exe 不只出现在 Windows XP 中，在使用 NT 内核的 Windows 系统中都会有 svchost.exe 的存在。一般在 Windows 2000 中 svchost.exe 进程的数目为 2 个，而在 Windows XP 中 svchost.exe 进程的数目就上升到了 4 个及 4 个以上，所以看到系统的进程列表中有几个 svchost.exe 不必惊慌，但也不要掉以轻心，因为有的病毒会千方百计地侵入 svchost.exe，对于这种情况是查看 svchost.exe 进程的执行路径。用户可以在系统中搜索 svchost.exe 文件的路径，正常的 svchost.exe 文件的存放路径应该在 C:\WINDOWS\System32 中 (C 为系统盘)。如果用户在其他目录下发现 svchost.exe 程序的话，那很可能就是中毒了。

spoolsv.exe：将文件加载到内存中以便迟后打印。

explorer.exe：这个进程主要负责显示系统桌面上的图标以及任务栏。

internat.exe：托盘区的拼音图标。

13.1.2 关闭系统的所有端口

如果在 Windows XP 中不需要开启端口，那么可以关闭系统的所有端口，其具体操作方法如下：

STEP 01 打开“网络连接”窗口

右击“网上邻居”图标，从弹出的快捷菜单中选择“属性”选项，弹出“网络连接”窗口。右击“本地连接”图标，从弹出的快捷菜单中选择“属性”选项，如下图所示。

STEP 02 打开“本地连接 属性”对话框

弹出“本地连接 属性”对话框，如下图所示。在“此连接使用下列项目”列表框中选择“Internet 协议 (TCP/IP)”选项，单击“属性”按钮。

基础知识

常用扫描与嗅探工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文件加密

远程攻击

木马攻防

聊天软件攻防

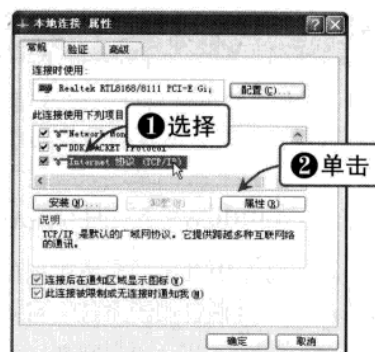
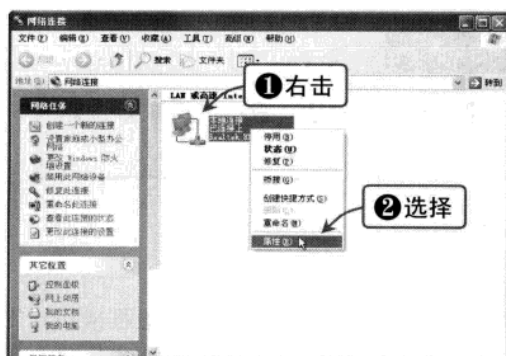
网页恶意代码攻防

电子邮件攻防

C 盘病毒攻防

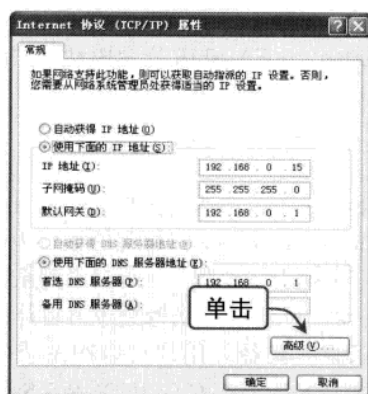
使用电脑安全软件

黑客攻防实用技巧



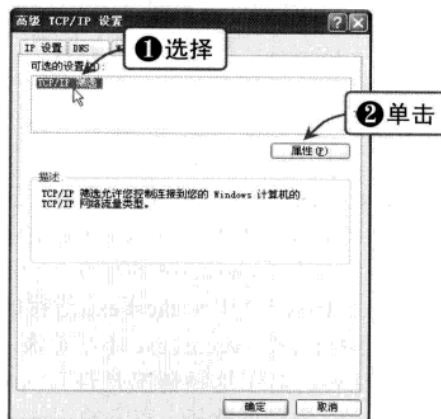
STEP 03 打开“Internet 协议 (TCP/IP) 属性”对话框

弹出“Internet 协议 (TCP/IP) 属性”对话框，单击“高级”按钮，如下图所示。



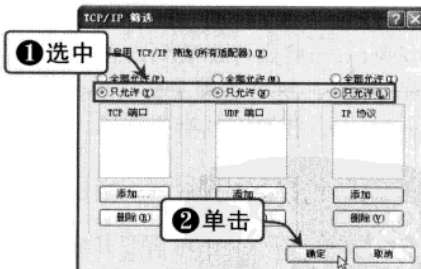
STEP 04 选择“TCP/IP 筛选”选项

弹出“高级 TCP/IP 设置”对话框，选择“选项”选项卡，在“可选的设置”列表中选择“TCP/IP 筛选”选项，单击“属性”按钮，如下图所示。



STEP 05 选择更新模式

弹出“TCP/IP 筛选”对话框，选中 3 个“只允许”单选按钮，然后单击“确定”按钮即可，如右图所示。



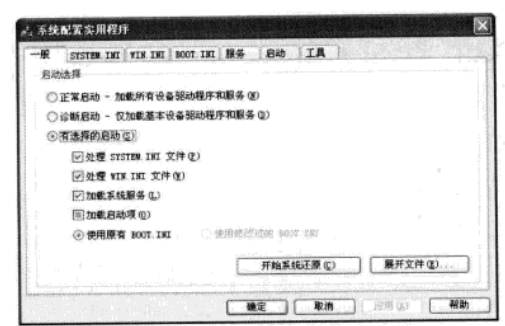
13.1.3 禁止随机启动程序

在系统中安装某些程序后，在重新启动电脑后会发现它们会自动启动，造成电脑启动速度减慢。另外，有些病毒也会随机启动，只要电脑一重新启动，它们就会自动启动，进而破坏系统正常运行。可以采用以下方法来禁止随机启动程序：

Chapter 13 黑客攻防实用技巧

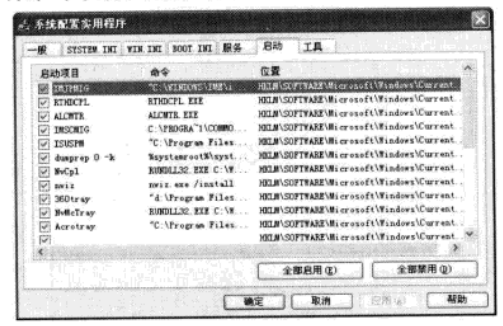
STEP 01 打开“系统配置实用程序”对话框

单击“开始”|“运行”命令，打开“运行”对话框，输入 msconfig 命令，按【Enter】键，弹出“系统配置实用程序”对话框，如下图所示。



STEP 02 禁用随机启动程序

选择“启动”选项卡，在其中取消选择需要随机启动的程序即可。此处的程序都不是系统的核心程序，大部分都可以禁用。禁用它们都不会造成系统无法启动的现象，但注意不要将杀毒软件随机启动程序禁用，如下图所示。

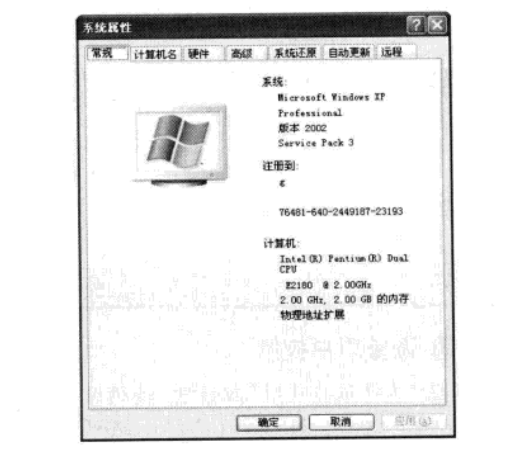


13.1.4 禁用远程协助功能

远程协助功能是 Windows XP 系统附带提供的一种简单的远程控制的方法。远程协助的发起者通过 MSN Messenger 向 Messenger 中的联系人发出协助要求，在获得对方同意后，即可进行远程协助。用户可以采用以下方法来禁用远程协助功能：

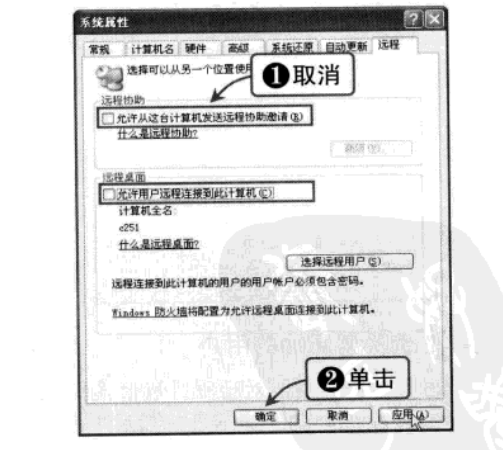
STEP 01 打开“系统属性”对话框

右击“我的电脑”图标，从弹出的快捷菜单中选择“属性”选项，弹出“系统属性”对话框，如下图所示。



STEP 02 禁用远程协助

选择“远程”选项卡，取消选择“允许从这台计算机发送远程协助邀请”和“允许用户远程连接到这台计算机”复选框，然后单击“确定”按钮即可，如下图所示。



13.1.5 设置注册表管理权限

在 Windows XP 中可以通过对不同的用户设置不同的访问注册表权限来保护注册表，这

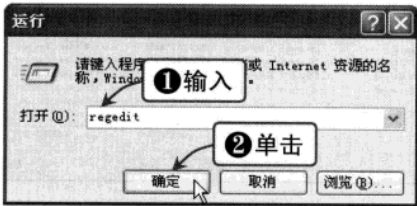
- 基础知
- 黑客
- 常用扫描
- 与嗅探工具
- 系统漏洞攻防
- Windows 系
- 设置系统
- 安全策略
- 系统与文
- 件加密
- 远程控
- 制攻防
- 木马
- 聊天软
- 件攻防
- 网页恶
- 意
- 电子邮
- 件攻防
- 病毒防
- 使用电
- 脑
- 安全软
- 件
- 黑客攻
- 防技巧



非常适合多用户共用一台电脑的情况，可以为使用这台电脑的每一位用户设置不同的注册表管理权限。设置注册表管理权限的具体操作步骤如下：

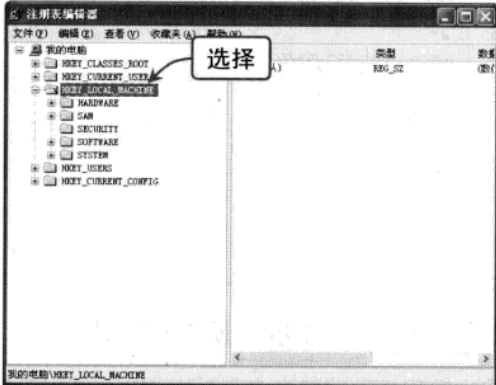
STEP 01 输入 regedit 命令

单击“开始”|“运行”命令，弹出“运行”对话框，在“打开”文本框中输入 regedit 命令，然后单击“确定”按钮，如下图所示。



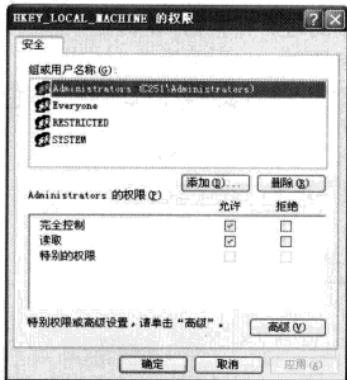
STEP 02 选择要设置管理权限的选项

打开“注册表编辑器”窗口，在该窗口中选择要设置管理权限的选项，在此以 HKEY_LOCAL_MACHINE 项为例，如下图所示。



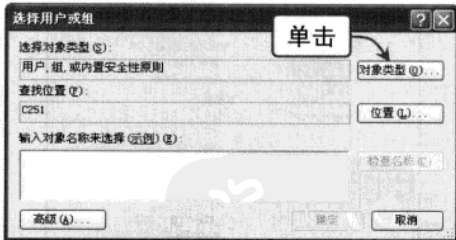
STEP 03 打开“HKEY_LOCAL_MACHINE 的权限”对话框

单击“编辑”|“权限”命令，打开“HKEY_LOCAL_MACHINE 的权限”对话框，如下图所示。



STEP 04 打开“选择用户或组”对话框

在“组或用户名称”列表中选择要设置管理权限的用户，如果要设置管理权限的用户不在其中，可以单击“添加”按钮，弹出“选择用户或组”对话框，单击“对象类型”按钮，如下图所示。



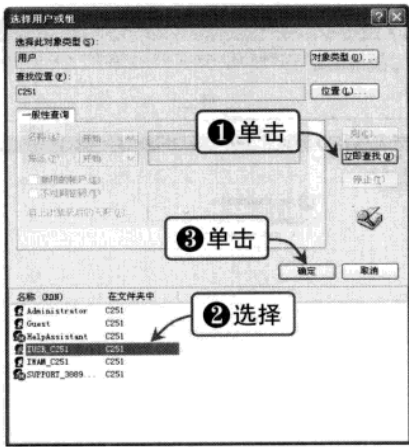
STEP 05 选择要添加的用户

弹出“选择类型”对话框，取消选择“内置安全性原则”和“组”复选框，然后单击“确定”按钮返回“选择用户或组”对话框。单击“高级”按钮，再单击“立即查找”按钮，在“名称”下方的列表中选择要添加的用户，单击“确定”按钮，如下图所示。

STEP 06 设置用户权限

返回“选择用户或组”对话框，继续单击“确定”按钮，返回“HKEY_LOCAL_MACHINE 的权限”对话框，所选用户就出现在“组或用户名称”中了。在此时的“HKEY_LOCAL_MACHINE 的权限”对话框中，根据自己的需要设置该用户相应的权限就可以了。

Chapter 13 黑客攻防实用技巧

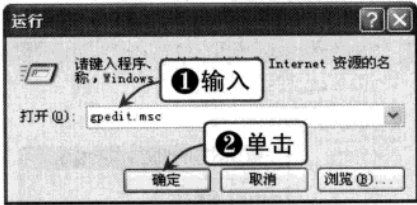


13.1.6 禁用组策略功能

组策略是 Windows XP 中一个非常有用的工具，与注册表一样，通过它可以对系统进行很多设置，但与注册表相比，使用它对系统进行设置既方便，又简洁，不需要像注册表那样需要一级一级地展开相应的项。如果要防止别人通过组策略对系统设置进行更改，可以禁用组策略功能。

STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，弹出“运行”对话框，输入 gpedit.msc 命令，单击“确定”按钮，如下图所示。

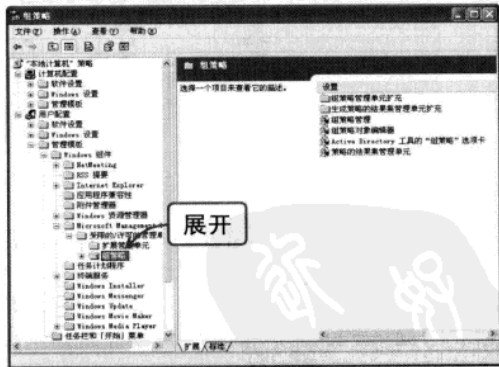


提示

在“运行”对话框的文本框中输入不同的命令，可以打开相应窗口。

STEP 02 展开“组策略”选项

打开“组策略”窗口，在该窗口左侧窗格中依次展开“用户配置”|“管理模板”|“Windows 组件”|“Microsoft Management Console”|“受限的/许可的管理单元”|“组策略”选项，如下图所示。



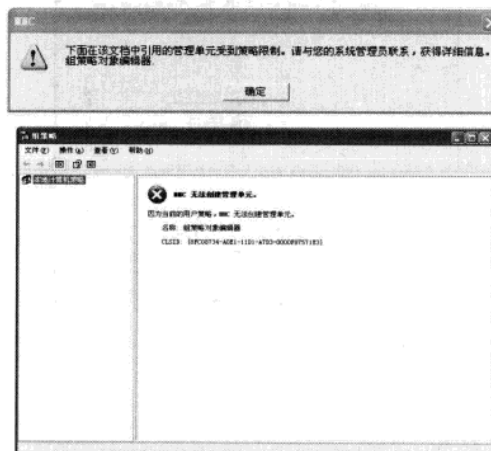
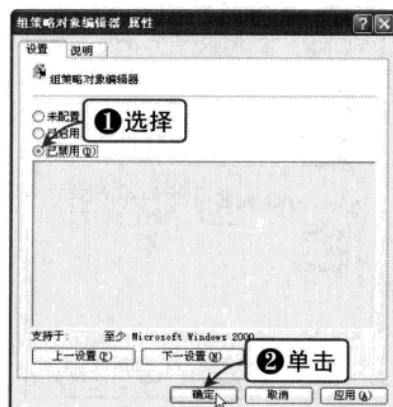
STEP 03 “组策略对象编辑器 属性”对话框

双击右侧窗格中的“组策略对象编辑器”选项，弹出“组策略对象编辑器 属性”对话框，在其中选中“已禁用”单选按钮，然后单击“确定”按钮，如下图所示。

STEP 04 阻止访问组策略

执行上述操作后，再次通过 gpedit.msc 命令启动组策略时，就会弹出 MMC 提示信息框，阻止访问组策略，如下图所示。

黑客
常用扫描
与嗅探工具
系统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
木马
聊天软
网页恶
代码攻
件攻
毒攻
安全软
黑客攻
防技巧



13.1.7 启用组策略功能

当组策略被禁用以后，可以通过以下方法来将此功能重新开启。

STEP 01 打开“注册表编辑器”窗口

打开“注册表编辑器”窗口，在左侧窗格中依次展开 HKEY_CURRENT_USER/Software/Policies/Microsoft/MMC/{8FC0B734-A0E1-11D1-A7D3-0000F87571E3} 项，如下图所示。

STEP 02 打开“编辑 DWORD 值”对话框

双击右侧窗格中的 Restrict_Run 选项，弹出“编辑 DWORD 值”对话框，在“数值数据”文本框中输入 0，然后单击“确定”按钮，如下图所示。完成以上设置后，运行 gpedit.msc 命令，即可顺利地进入到组策略中了。



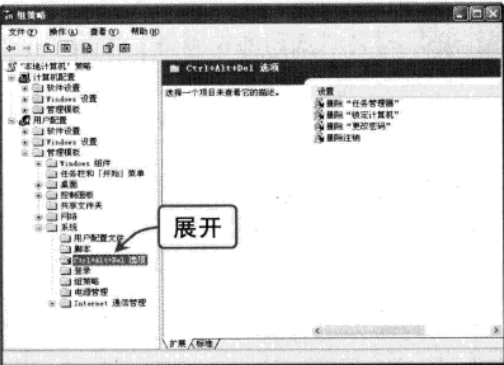
13.1.8 禁用“Windows 任务管理器”

“Windows 任务管理器”工具在 Windows XP 中也非常重要，可以采用以下方法将其禁用。

Chapter 13 黑客攻防实用技巧

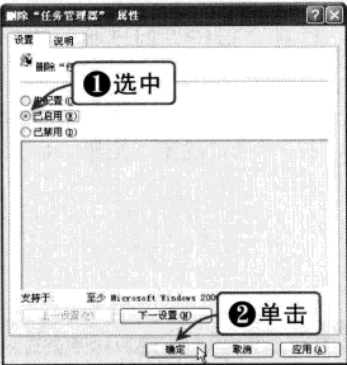
STEP 01 打开“组策略”窗口

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 gpedit.msc 命令，然后按【Enter】键，打开“组策略”窗口。在左侧窗格中依次展开“‘本地计算机’策略”|“用户配置”|“管理模板”|“系统”|“Ctrl+Alt+Del 选项”选项，如下图所示。



STEP 02 打开“删除‘任务管理器’属性”对话框

双击右侧窗格中的“删除‘任务管理器’”选项，弹出“删除‘任务管理器’属性”对话框，选中“已启用”单选按钮，单击“确定”按钮，如下图所示。完成以上设置后，运行 gpedit.msc 命令，即可禁用“Windows 任务管理器”。

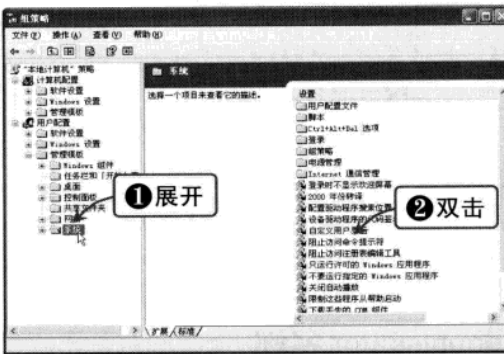


13.1.9 禁用的命令提示符

禁用“命令提示符”窗口的具体操作步骤如下：

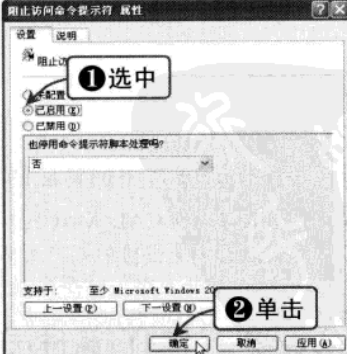
STEP 01 打开“组策略”窗口

打开“组策略”窗口，在左侧窗格中依次展开“用户配置”|“管理模板”|“系统”选项，如下图所示。双击右侧窗格中的“阻止访问命令提示符”选项，



STEP 02 打开“阻止访问命令提示符 属性”对话框

弹出“阻止访问命令提示符 属性”对话框，选中“已启用”单选按钮，单击“确定”按钮，如下图所示。完成以上设置后，运行 gpedit.msc 命令，即可禁用“命令提示符”窗口。



- 基础知识
- 黑客
- 常用扫描
- 与嗅探工具
- 系统漏洞攻防
- 设置系统
- 安全策略
- 系统与文
- 件加密
- 远程控
- 制攻防
- 木马
- 聊天软
- 件攻防
- 网页恶
- 意代码
- 攻防
- 电子邮
- 件攻防
- C盘病
- 毒攻防
- 使用电
- 脑安全
- 软件
- 黑客攻
- 防实
- 用技
- 巧



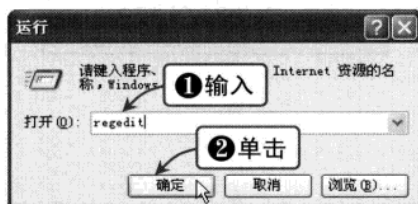
13.1.10 找出系统隐藏的超级用户

对于一些比较高明的黑客，可以通过修改注册表等手段（修改注册表 HKEY_LOCAL_MACHINE\SAM 子键）创建隐藏的超级用户，并且在账户管理器看不到这个用户；在“命令提示符”窗口中使用 net share 命令也看不到。如何找到这个隐藏的系统用户呢？

由于黑客在创建隐藏的超级用户时修改了 HKEY_LOCAL_MACHINE\SAM 子键，因此只要用户将事先备份好的该子键与当前同一子键相对照，就能发现隐藏的账户。将备份的子键导入注册表，即可清除隐藏账户，具体操作方法如下：

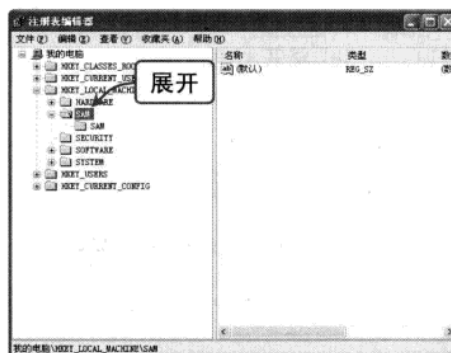
STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，弹出“运行”对话框，在该对话框的“打开：”文本框中输入 regedit 命令，单击“确定”按钮，如下图所示。



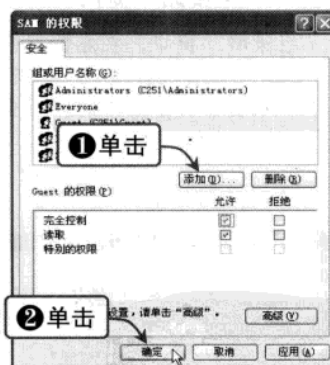
STEP 02 打开“注册表编辑器”窗口

打开“注册表编辑器”窗口，在该窗口的左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SAM 分支，如下图所示。



STEP 03 打开“SAM 的权限”对话框

右击 SAM 子键，从弹出的快捷菜单中选择“权限”选项，弹出“SAM 的权限”对话框，单击“添加”按钮添加账户，并设置该账户权限为完全控制，单击“确定”按钮，如右图所示。



STEP 04 查看 Name 子键下面对应的当前的账户列表

分别展开 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names 的分支，Name 子键下面对应的就是当前的账户列表。用户可以事先将 HKEY_LOCAL_MACHINE\SAM 导出备份，检查时再导出一次，对照两者的不同，就可以发现隐藏的超级用户了。

13.1.11 改变计算机管理员账户 Administrator 名称

除了给计算机管理员账户 Administrator 设置密码提高安全性外，还可以改变计算机管理

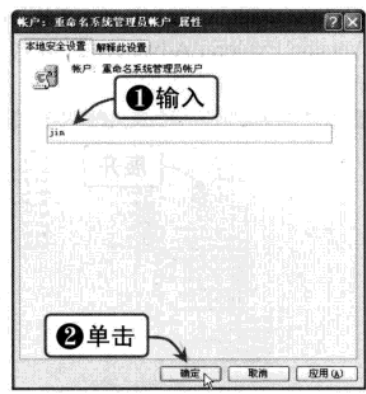
Chapter 13 黑客攻防实用技巧

员账户 Administrator 的名称，这也是提高系统安全的一个方法。具体操作方法如下：

- STEP 01** 打开“本地安全设置”窗口

在“本地安全设置”窗口中依次展开“本地策略”|“安全选项”选项，双击右侧窗格中的“账户：重命名系统管理员账户”选项，如下图所示。
- STEP 02** 打开“账户：重命名系统管理员账户 属性”对话框

弹出“账户：重命名系统管理员账户 属性”对话框，输入 Administrator 的名称，完成后单击“确定”按钮即可，如下图所示。



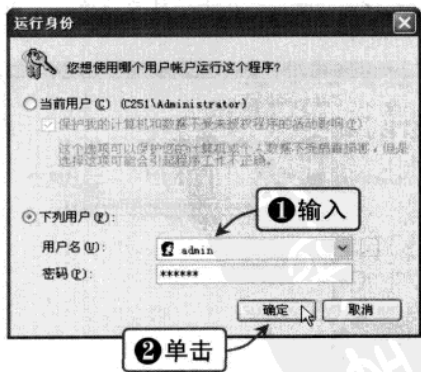
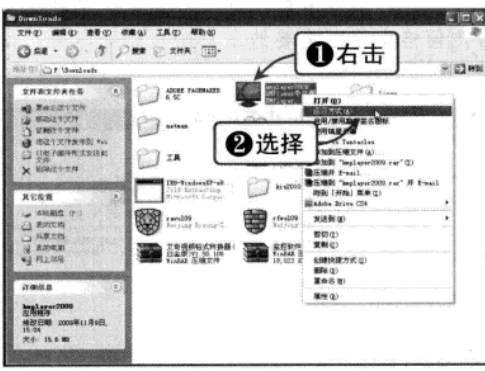
13.1.12 为自己分配管理员权限

安装在 Windows XP 中的许多程序都要求用户具有一定的管理权限才能使用，因此为了能够使用好程序，有时需要为自己临时分配一个访问程序的管理权限。为自己分配管理员权限的具体操作步骤如下：

- STEP 01** 选择“运行方式”选项

在分配管理权限时，可以先以普通用户身份登录到 Windows XP 系统中，按住【Shift】键的同时右击程序安装文件，在弹出的快捷菜单中选择“运行方式”选项，如下图所示。
- STEP 02** “运行身份”对话框

弹出“运行身份”对话框，选中“下列用户”单选按钮，在“用户名”和“密码”文本框中输入相应的用户名和密码后，单击“确定”按钮，就可以以该用户运行该安装程序了，如下图所示。



13.1.13 让系统文件彻底不显示

用户为文件设置“隐藏”属性后，通过单击“工具”|“文件夹选项”命令打开“文件

基础
知识
黑客
常用
扫描
与嗅探
工具
统漏洞
攻防
安全策
略
设置系
统
系统与
文
件加密
远程
控制
攻
防
木马
聊天
软
网
页
恶
意
电
子
邮
C
盘
病
使用
电脑
黑客
攻
防



夹选项”对话框，然后在“查看”选项卡中选中“显示所有文件”单选按钮，即可看到被隐藏的文件。要想彻底隐藏系统文件，可以使用下面的方法进行操作。

STEP 01 展开 SHOWALL 分支

在“运行”对话框中输入 regedit 命令并按【Enter】键，打开“注册表编辑器”窗口，然后在左侧窗格中依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL 分支，如下图所示。



STEP 02 编辑 DWORD 值

新建或选中名为 CheckValue (REG_DWORD 类型) 的键值项，将其键值设置为 1，单击“确定”按钮，重新启动计算机即可，如下图所示。



13.1.14 删除无关用户账户

系统在安装好后，会默认创建一些用户和组，如 Guest、HwlpAssistant 及 Support_38-8945a0 等用户账户。虽然这些内置账户在特定的环境中会使用到，不过它们更多地是被黑客所利用，对系统造成巨大的威胁。如果是无特殊需求的用户，最好禁用它们，具体操作方法如下：

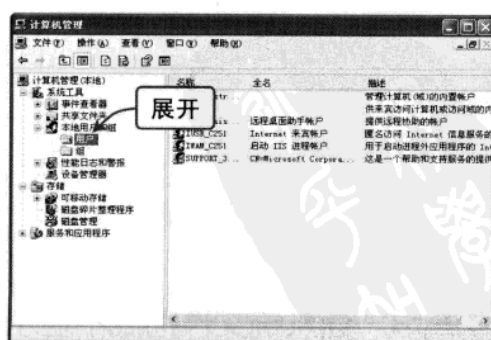
STEP 01 打开“管理工具”窗口

单击“开始”|“控制面板”命令，打开“控制面板”窗口，双击“管理工具”图标，打开“管理工具”窗口，双击“计算机管理”图标，如下图所示。



STEP 02 删除无关账户

打开“计算机管理”窗口，在左侧窗格中依次展开“本地用户和组”|“用户”选项，在右侧窗格中将不需要的用户账户删除即可，如下图所示。



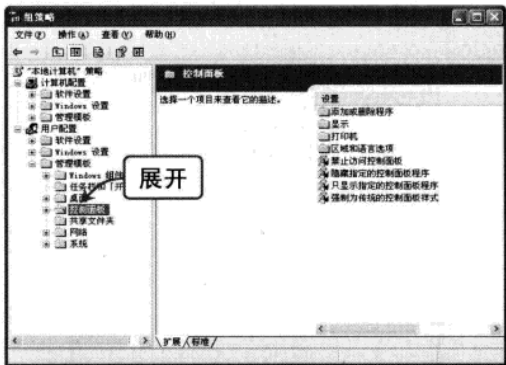
Chapter 13 黑客攻防实用技巧

13.1.15 禁止访问“控制面板”

“控制面板”在 Windows XP 中是一个非常重要的管理工具，通过它可以对系统的绝大部分设置进行修改。禁止访问“控制面板”的具体操作方法如下：

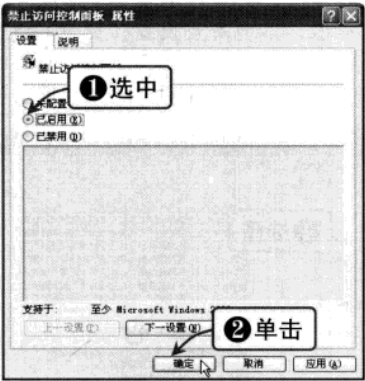
STEP 01 打开“组策略”窗口

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 gpedit.msc 命令，然后按【Enter】键，打开“组策略”窗口。在该窗口的左侧窗格中依次展开“用户配置”|“管理模板”|“控制面板”选项，如下图所示。



STEP 02 “禁止访问控制面板 属性”对话框

双击右侧窗格中的“禁止访问控制面板”选项，在弹出的“禁止访问控制面板 属性”对话框中选中“已启用”单选按钮，然后单击“确定”按钮，如下图所示。

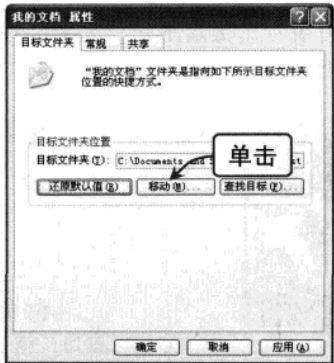


13.1.16 将“我的文档”转移到非系统分区

默认情况下，保存文件时一般会保存到“我的文档”中，而“我的文档”存放在系统分区里，时间久了会使系统盘容量减少，而且当格式化系统分区时，“我的文档”中保存的内容也会受到影响。因此可以将“我的文档”文件夹转移到非系统分区中，以解决上述问题。

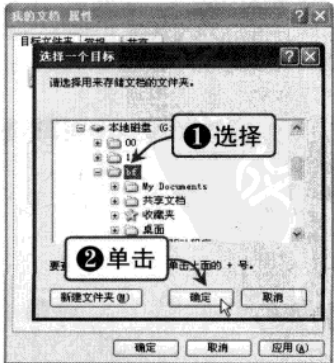
STEP 01 打开“我的文档 属性”对话框

右击“我的文档”图标，从弹出的快捷菜单中选择“属性”选项，弹出“我的文档 属性”对话框，单击“移动”按钮，如下图所示。



STEP 02 查看漏洞防护

在弹出的“选择一个目标”对话框中设置文件夹的路径，然后依次单击“确定”按钮即可，如下图所示。



基础
知识
与
工
具
常用
扫描
工具
统
漏
洞
防
攻
安
全
策
略
系
统
与
文
件
加
密
远
程
控
制
防
攻
木
马
防
防
件
攻
防
网
页
恶
意
代
码
攻
防
电
子
邮
件
攻
防
C
盘
病
毒
攻
防
安
全
软
件
黑
客
攻
防
实
用
技
巧



13.2 系统应用与故障排除技巧

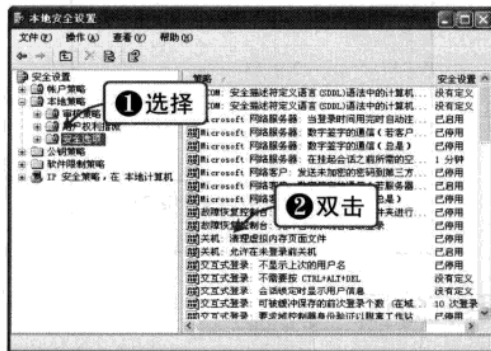
下面将详细介绍 Windows XP 的一些应用技巧及常见故障排除方法。

13.2.1 关机时清空页面文件

实现关机时清空页面文件的具体操作步骤如下：

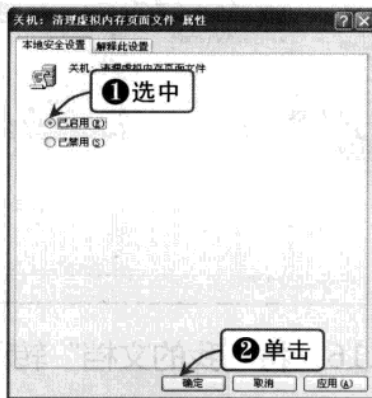
STEP 01 选择“安全选项”选项

打开“控制面板”窗口，双击“管理工具”图标，在弹出的窗口中双击“本地安全策略”图标，弹出“本地安全设置”窗口，选择“本地策略”|“安全选项”选项，如下图所示。双击“关机：清理虚拟内存页面文件”属性选项。



STEP 02 选中“已启用”单选按钮

在弹出的对话框中选中“已启用”单选按钮，然后单击“确定”按钮即可，如下图所示。

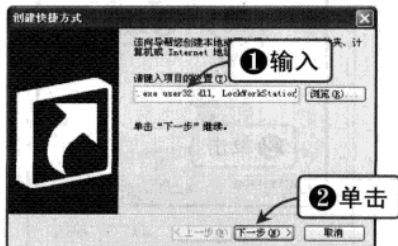


13.2.2 创建锁定计算机的快捷方式

因有急事而要离开，但又不希望电脑进行系统注销时可以通过双击桌面快捷方式来迅速锁定键盘和显示器，且无需使用【Ctrl+Alt+Del】组合键或屏幕保护程序。

STEP 01 启动创建快捷方式向导

右击桌面空白处，在快捷菜单中选择“新建”|“快捷方式”选项，接着系统便会启动创建快捷方式向导。在文本框中输入下列命令：rundll32.exe user32.dll, LockWorkStation，单击“下一步”按钮，如下图所示。



STEP 02 输入快捷方式名称

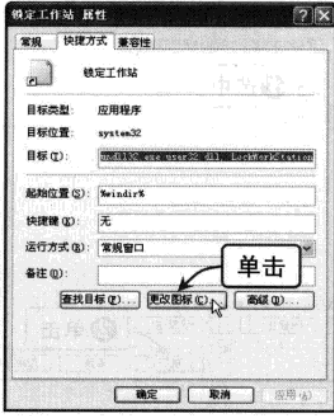
在弹出的窗口中输入快捷方式名称，可将其命名为“锁定工作站”，或选用自己所喜欢的任何名称，然后单击“完成”按钮，如下图所示。



Chapter 13 黑客攻防实用技巧

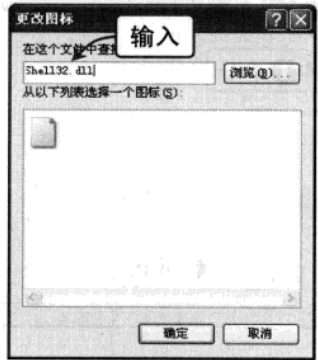
STEP 03 单击“更改图标”按钮

右击快捷方式图标，并在随后出现的快捷菜单中选择“属性”选项，在弹出的对话框中选择“快捷方式”选项卡，接着单击“更改图标”按钮，如下图所示。



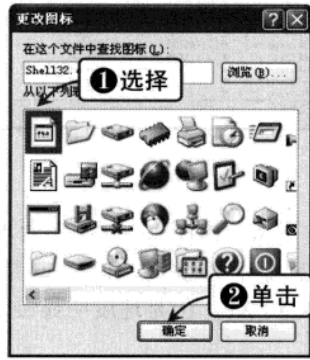
STEP 04 输入 Shell32.dll

在弹出的“更改图标”对话框的文本框中输入 Shell32.dll，如下图所示。



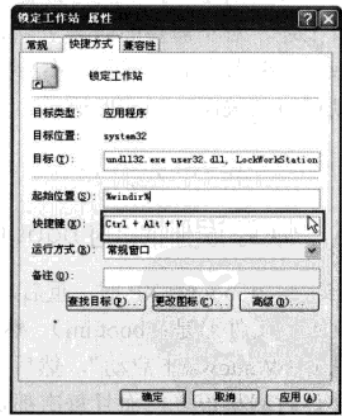
STEP 05 选择所需图标

从列表中选择所需图标，并单击“确定”按钮，如下图所示。



STEP 06 添加快捷键组合

右击快捷方式图标，并在弹出的快捷菜单中选择“属性”选项，在弹出的对话框中选择“快捷方式”选项卡，在“快捷键”文本框中输入任何键值，而 Windows XP 则会将其转换成快捷键组合（一般应采取【Ctrl+Alt+任意键】的形式），如下图所示。



13.2.3 关闭 Windows XP 的自动播放功能

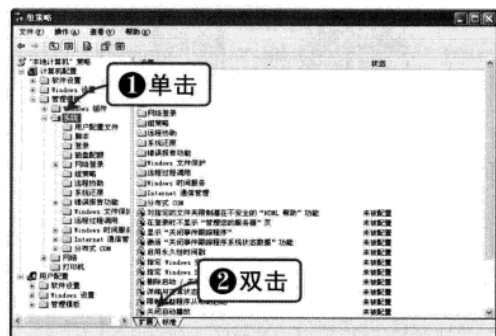
有时用户将多媒体光盘插入驱动器后光盘会自动播放，这称为 Windows XP 的自动播放功能。用户可以使用下面介绍的办法关闭这个功能。

黑客
基础知识
常用扫描
与嗅探工具
Windows 系
统漏洞攻防
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶意
代码攻防
电子邮
件攻防
C 盘病
毒攻防
使用电脑
安全软件
黑客攻防



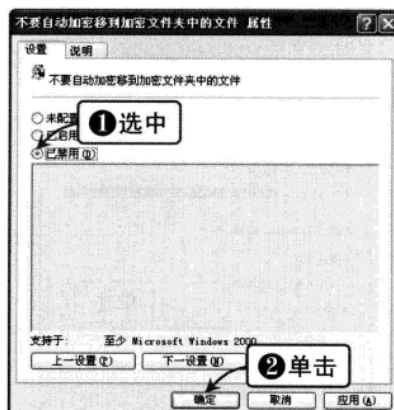
STEP 01 选择“安全选项”选项

单击“开始”|“运行”命令，在弹出的对话框中输入 gpedit.msc 命令，单击“确定”按钮。在弹出的“组策略”窗口中依次选择“计算机配置”|“管理模板”|“系统”选项，双击“关闭自动播放”选项，如下图所示。



STEP 02 选中“已禁用”单选按钮

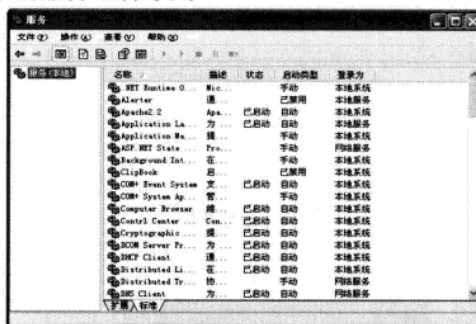
在弹出对话框的“设置”选项卡中，选中“已禁用”单选按钮，最后单击“确定”按钮即可，如下图所示。



13.2.4 自行配置 Windows XP 的服务

如果用户是单机使用 Windows XP，那么很多服务组件是根本不需要的，额外的服务程序反而会影响系统的速度，完全可将这些多余的服务组件禁用。

在“控制面板”中双击“管理工具”图标，在弹出的窗口中双击“服务”图标，在弹出的服务列表窗口中可以看到有些服务已经启动，有些则没有。用户可查看相应的服务项目描述，对不需要的服务予以关闭。如 Alerter，如果未连上局域网且不需要管理警报，则可将其关闭，如右图所示。



13.2.5 恢复误删除的 boot.ini 文件

第一次装 Windows XP 时，重启后没有任何问题。但是由于误操作，删掉了 C 盘目录下的一个文件（文件名是：boot.ini），然后再重启时，每次都显示两行字：“boot.ini 是非法的。现在正从 C:/Windows/下启动”，然后可以顺利进入 Windows XP。但是速度明显慢了，比删除这个文件时慢了很多，而且每次都要看见这两行字。

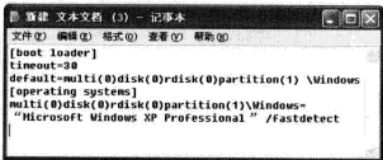
boot.ini 是系统启动时，需要查询的一个系统文件，它告诉启动程序本电脑有几个操作系统、各系统的位置在哪里等信息。

重新恢复的方法如下：单击“开始”|“程序”|“附件”|“记事本”命令，打开“记事本”程序，在“记事本”窗口中输入：

Chapter 13 黑客攻防实用技巧

```
[boot loader]
Timeout=30
default=multi (0) disk (0) rdisk (0) partition (1) \Windows
[operating systems]
Multi (0) disk (0) rdisk (0) partition (1) \Windows= "Microsoft Windows XP Professional" /fastdetect
```

然后将它保存为名字是 boot.ini 的文件，并将此文件保存到 C 盘的根目录下即可，如右图所示。



13.2.6 自动关闭停止响应的程序

在 Windows XP 操作系统中，自动关闭停止响应的程序设置使 Windows XP 当检测到某个应用程序已经停止响应时，可以自动关闭它，而不需要进行麻烦的手工干预。

STEP 01 打开注册表编辑器

单击“开始”|“运行”命令，在弹出的对话框中输入 regedit 命令，单击“确定”按钮，打开注册表编辑器，展开 HKEY_CURRENT_USER\Control Panel\Desktop 分支，如下图所示。



STEP 02 设置键值

在右侧窗格中找到 AutoEndTasks 键值项，双击此选项，在弹出的“编辑字符串”对话框中将其键值设置为 1，单击“确定”按钮即可，如下图所示。



13.2.7 删除 Windows XP 的“更新”选项

对于大多数的用户来说，Windows XP 的 Windows Update 功能似乎作用不大，可以将其去掉，其具体操作步骤如下：

STEP 01 新建 DWORD 键值项

打开注册表编辑器，展开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 子键分支，单击“编辑”|“新建”命令，新建一个类型为 DWORD 的值，名称为 NoCommonGroups，如下图所示。

STEP 02 设置键值

双击新建的 NoCommonGroups 子键，弹出“编辑字符串”对话框，在“编辑字符串”文本框中输入键值 1，然后单击“确定”按钮并重新启动系统即可，如下图所示。

基础知识

与嗅探工具

系统漏洞攻防

安全策略

系统与安全

远程控制

木马

聊天软件

网页攻击

代码攻击

电子邮件

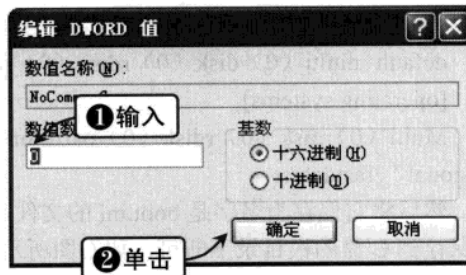
攻击

使用电脑

安全软件

黑客攻防

实用技巧



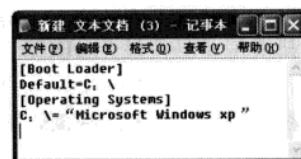
13.2.8 恢复被破坏的系统引导文件

电脑只安装了 Windows XP 系统，在开机时显示“BOOT.INI 非法，正从 C:\WINDOWS\启动”，然后就进入了启动状态，并且也能照样工作。

出现这种情况是因为 C 盘下面的 Boot.ini 文件被破坏了。但是，由于用户的机器中只有一个操作系统，当然它就是默认的操作系统，即使 Boot.ini 文件被破坏了，也将自动地引导该系统进行装载。

解决的办法是建立一个 Boot.ini 文件，其内容为：

```
[Boot Loader]
Default=C:\
[Operating Systems]
C:\="Microsoft Windows xp"
```

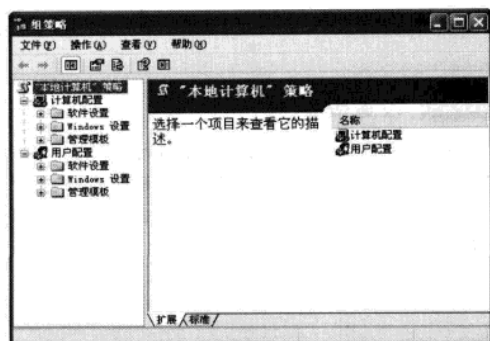


13.2.9 无法打开注册表

恶意程序利用注册表修改了 IE 浏览器的首页后，为了防止用户使用注册表进行修复会禁止使用注册表，当执行这一命令时系统会弹出一个提示信息框提示“注册表编辑已被管理员禁用”，解决方法如下：

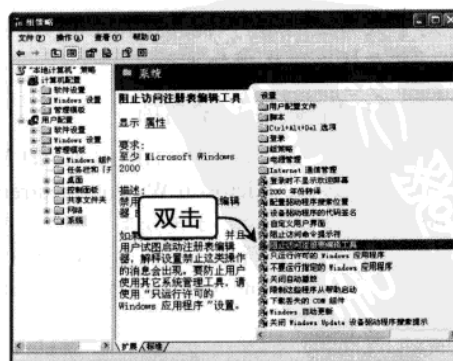
STEP 01 打开“组策略”窗口

在“运行”对话框中输入 gpedit.msc 命令，按【Enter】键，打开“组策略”窗口，如下图所示。



STEP 02 阻止访问注册表编辑工具

依次展开“用户配置”|“管理模板”|“系统”选项，双击右窗格中的“阻止访问注册表编辑工具”选项，如下图所示。



Chapter 13 黑客攻防实用技巧

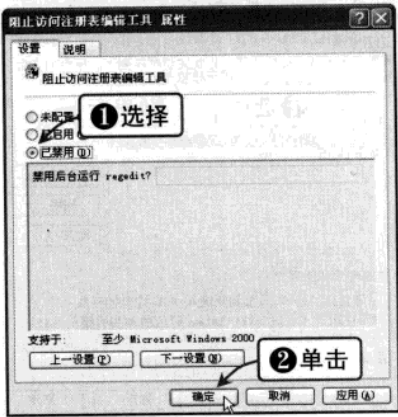
STEP 03 单击“已禁用”单选按钮

在弹出的“阻止访问注册表编辑工具”对话框中选中“已禁用”单选按钮，单击“确定”按钮后，再退出“组策略”窗口即可，如右图所示。



提示

禁用“阻止访问注册表编辑工具”策略后，用户就可以访问注册表编辑器了。

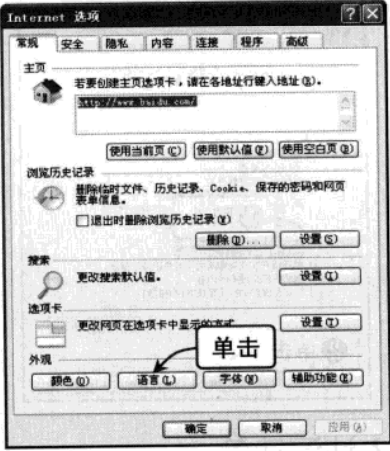


13.2.10 将自动更新页面改为中文

系统为 Windows XP 中文版，使用 Windows Update 时发现界面为英文的，怎样才能将此界面改为中文？具体操作方法如下：

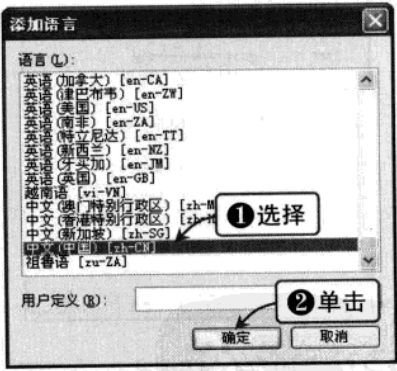
STEP 01 打开“Internet 选项”对话框

打开 IE 浏览器窗口，单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框，单击“语言”按钮，如下图所示。



STEP 02 添加语言

在弹出的“语言首选项”对话框中单击“添加”按钮，在弹出的“添加语言”对话框的“语言”列表框中选择“中文（中国）[zh-CN]”选项，单击“确定”按钮，如下图所示。



STEP 03 移动语言选项

返回“语言首选项”对话框，然后选择“中文（中国）[zh-CN]”选项，单击右侧的“上移”按钮，将“中文（中国）[zh-CN]”选项移动到最上面，如下图所示。

STEP 04 单击“确定”按钮

依次单击“确定”按钮，关闭对话框，然后重新启动电脑即可。

基础知识

与嗅探工具

Windows 系统

设置系统

安全策略

件加密

系统与安全

远程控制

攻防

木马

聊天软件

网页恶意

代码攻防

件攻防

电子邮箱

毒攻防

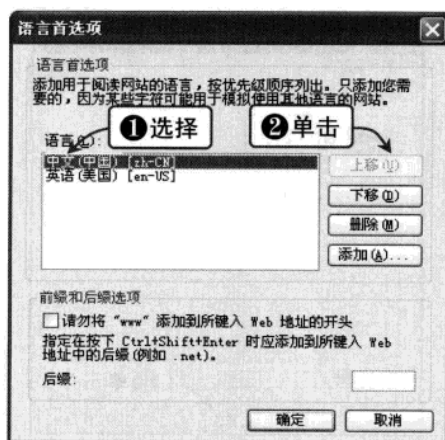
C 盘病毒

使用电脑

安全软件

黑客攻防

实用技巧



提示

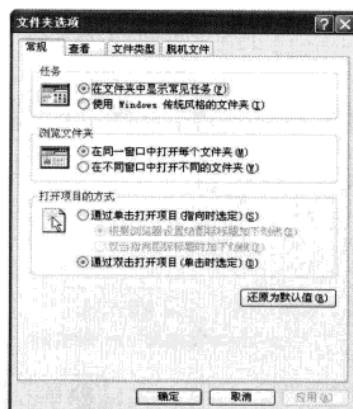
通过将“语言首选项”设置为中文，可以将 Windows Update 自动更新页面改为中文显示。

13.2.11 无法设置共享文件的访问权限

安装 Windows XP 操作系统后，发现无法对共享文件设置访问权限，解决方法如下：

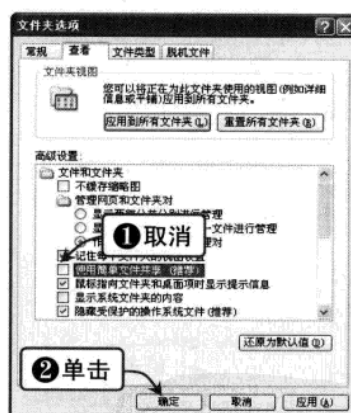
STEP 01 打开“文件夹选项”对话框

在桌面上双击“我的电脑”图标，打开“我的电脑”窗口，单击“工具”|“文件夹选项”命令，弹出“文件夹选项”对话框，如下图所示。



STEP 02 取消简单文件共享功能

选择“查看”选项卡，在“高级设置”列表框中取消选择“使用简单文件共享”复选框，如下图所示。单击“确定”按钮应用上述设置，即可取消简单文件共享功能。



13.2.12 恢复 Windows XP 系统的输入法浮动条

恢复 Windows XP 系统的输入法浮动条的具体操作步骤如下：

STEP 01 打开“区域和语言选项”对话框

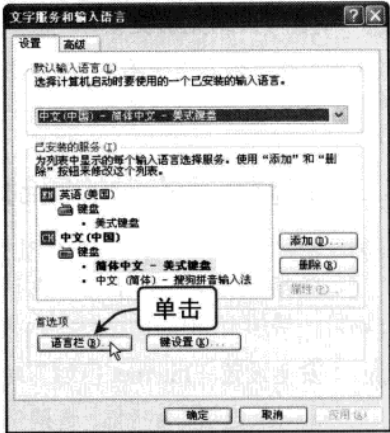
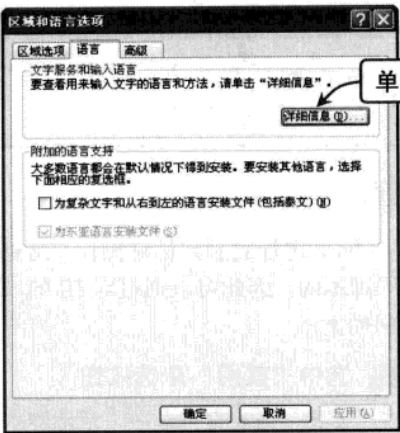
打开“控制面板”窗口，双击“区域和语言选项”图标，在弹出的对话框中选择“语言”选项卡，单击其中的“详细信息”按钮，如下图所示。

STEP 02 单击“语言栏”按钮

弹出“文字服务和输入语言”对话框，选择“设置”选项卡，在“首选项”选项区中单击“语言栏”按钮，如下图所示。

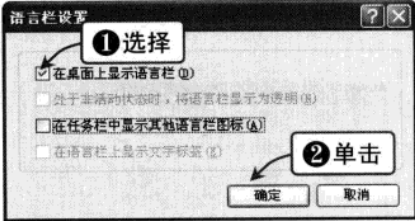
免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 13 黑客攻防实用技巧



STEP 03 打开“语言设置栏”对话框

弹出“语言栏设置”对话框（如右图所示），选中“在桌面上显示语言栏”复选框，单击“确定”按钮，关闭此对话框，然后依次单击“确定”按钮即可。



13.3 IE 浏览器安全应用技巧

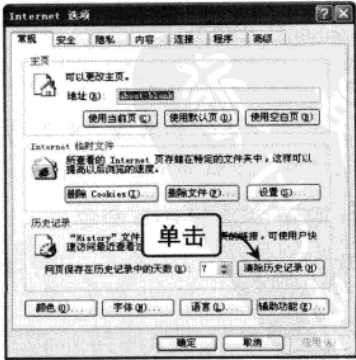
IE（Internet Explorer）浏览器是 Windows 操作系统自带的一种网络浏览软件，一般用户都使用它来与服务器沟通，以达到数据交换与显示的目的。下面将介绍 IE 浏览器安全应用技巧。

13.3.1 清除地址栏中浏览过的网址和中文实名地址

在地址栏使用网络实名搜索并浏览相关网站后，常常会在地址栏中留下这些网址和中文实名地址，这样很容易将个人隐私泄露。在默认设置状态下，地址栏中将保留浏览过的网址和中文名地址，通过 Internet 的属性设置可以将其清除，其具体操作步骤如下：

STEP 01 打开控制面板

打开 IE 浏览器，单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框。在“常规”选项卡中单击“历史记录”选项区中的“清除历史记录”按钮，如右图所示。



黑客
基础知识
常用扫描
与嗅探工具
系统漏洞攻防
Windows 系
统漏洞攻防
安全策略
设置系统
安全策略
系统与文
件加密
远程控
制攻防
木马
聊天软
件攻防
网页恶
意代码攻
防
电子邮
件攻防
病毒防
御
使用电
脑安全
黑客攻
防技巧



STEP 02 清除网页浏览历史记录

在弹出的提示信息框中单击“是”按钮，即可清除地址栏中浏览过的网页历史记录，如右图所示。

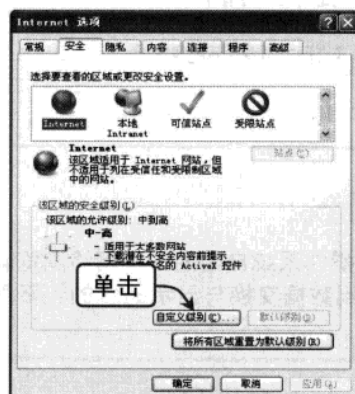


13.3.2 恢复鼠标右键的复制和粘贴功能

在浏览网页时，单击鼠标右键不能弹出快捷菜单对网页进行复制和粘贴操作。这是有些网页使用了防复制的脚本，而 IE 在默认情况下是启用脚本的，因此可以通过对 IE 的安全性进行调整，禁用 IE 中的活动脚本，其具体操作步骤如下：

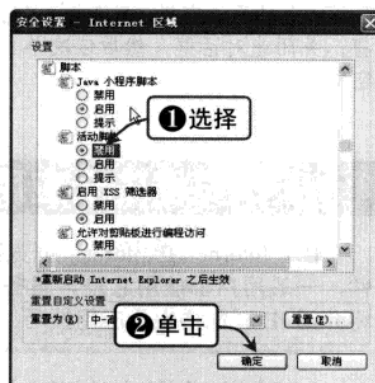
STEP 01 “安全设置—Internet 区域”对话框

打开“Internet 选项”对话框，选择“安全”选项卡，单击“自定义级别”按钮，弹出“安全设置—Internet 区域”对话框，如下图所示。



STEP 02 选中“禁用”单选按钮

在“设置”列表框中选中“活动脚本”项下的“禁用”单选按钮（如下图所示），单击“确定”按钮，在弹出的提示信息框中单击“是”按钮。



提示



还可使用鼠标右键的方法，即右击，此时该网页中将弹出一个提示信息框，一直按住鼠标右键不放，同时使用鼠标左键单击提示信息框中的“确定”按钮，然后再释放鼠标右键，即可使用鼠标右键的功能了。

13.3.3 恢复 IE 浏览器默认首页

IE 窗口的标题栏被改成“欢迎访问……网站”的样式，通过修改注册表即可解决该故障，其具体操作步骤如下：

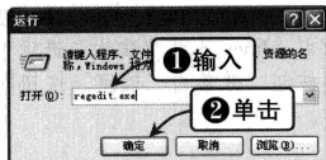
STEP 01 输入 regedit.exe 命令

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit.exe 命令，单击“确定”按钮，如下图所示。

STEP 02 打开“注册表编辑器”窗口

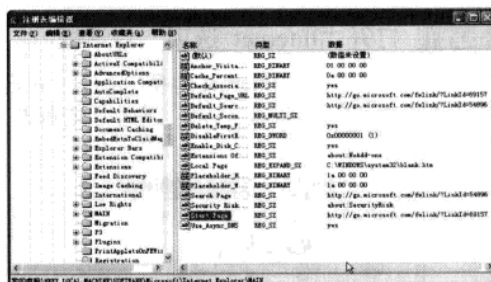
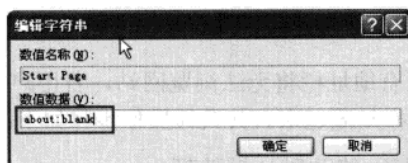
打开“注册表编辑器”窗口，找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main 目录，如下图所示。

Chapter 13 黑客攻防实用技巧



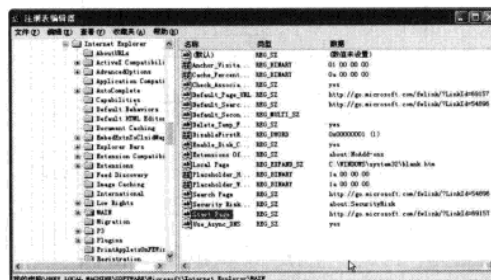
STEP 03 改为 about:blank

将窗口右边的 Start Page 字符串的数值改为 about:blank，如下图所示。



STEP 04 更改字符串

按照同样的方法找到 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main 目录，将窗口右边的 Start Page 字符串的数据改为 about:blank，完成后重新启动计算机即可，如下图所示。

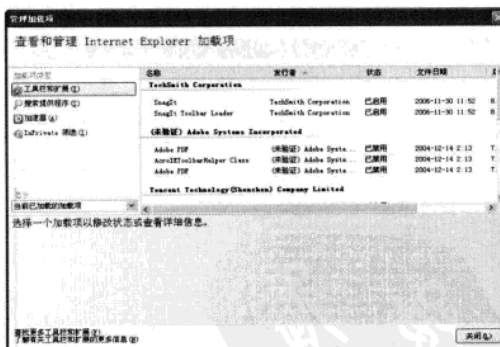


13.3.4 管理 Internet 加载项

Internet 加载项向 IE 中添加了多种功能（如工具栏和按钮等），这会使浏览更加有趣或高效。大多数加载项在下载安装之前必须获得用户的授权，但有些加载项可能会未经用户同意即进行加载。当然，还有一些加载项是随 Windows 安装的。

在 Internet Explorer 中管理加载项的方法是：在 IE 窗口中单击“工具”|“管理加载项”命令，弹出“管理加载项”对话框，如右图所示。

如果某加载项导致网页不能正常显示或被迫关闭，并弹出崩溃报告检测到加载项问题，则可以在“加载管理器”对话框中禁用该加载项。



13.3.5 设置 IE 浏览器拒绝运行 Java 小程序脚本

设置 IE 浏览器拒绝运行 Java 小程序脚本能在一定程度上提高系统安全性，其设置的具体操作方法如下：

基础知识

常用扫描与嗅探工具

Windows 系统漏洞攻防

设置系统安全策略

系统与文件加密

远程控制攻防

木马聊天软件攻防

网页恶意代码攻防

电子邮箱攻防

病毒攻防

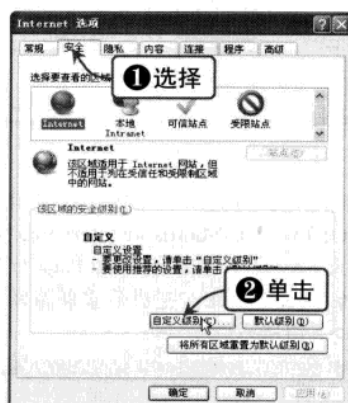
使用电脑安全软件

黑客攻防实用技巧



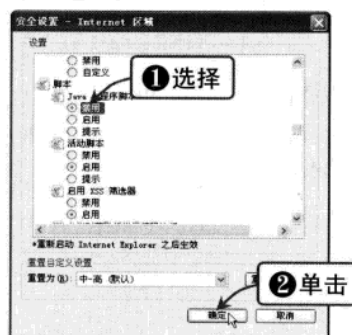
STEP 01 打开“Internet 选项”对话框

单击“工具”|“Internet 选项”命令，弹出“Internet 选项”对话框，选择“安全”选项卡，单击“自定义级别”按钮，如下图所示。



STEP 02 选中“禁用”单选按钮

弹出“安全设置”对话框，在“设置”列表框中选中“Java 小程序脚本”选项下的“禁用”单选按钮，并单击“确定”按钮即可，如下图所示。



13.3.6 隐藏 IE 地址栏

IE 地址栏是用户进入网站的必经之路，如果没有地址栏将无法浏览网站。若用户不想让其他用户使用 IE 地址栏来浏览网站，可以将地址栏隐藏起来。其具体操作步骤如下：

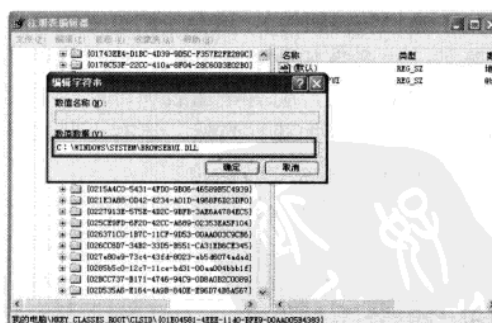
STEP 01 打开“注册表编辑器”窗口

打开“注册表编辑器”窗口，依次展开 HKEY_CLASSES_ROOT\CLSID\{01E04581-4EEE-11d0-BFE9-00AA005B4383}\InProcServ-er 32 分支，如下图所示。



STEP 02 修改默认键值项

在右侧窗口中选中默认（REG_SZ 类型）键值项，将其键值随意进行修改即可（默认情况下是 C:\WINDOWS\SYSTEM\BROWSERUI.DLL），如下图所示。



提示

设置完成后重新打开 IE 浏览器，即可发现 IE 地址栏被隐藏。需要注意的是，在注册表中的设置有的可以直接生效，有的则需要注销一下，有的需要重新启动电脑才能生效。

13.3.7 解除 IE 的分级审查口令

当 IE 被设置了分级审查口令后，如果忘记了密码，那么即使重新安装 IE 也不能将口令去除。要想解除分级审查口令，可以采用以下方法进行操作：

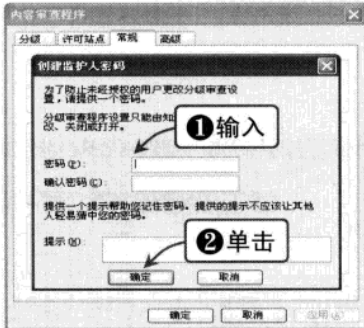
STEP 01 打开“注册表编辑器”窗口

单击“开始”|“运行”命令，在弹出的“运行”对话框中输入 regedit 命令，并按【Enter】键，打开“注册表编辑器”窗口。依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings 分支，删除 key 子键，如下图所示。



STEP 02 “创建监护人密码”对话框

重新启动 IE 后单击“工具”|“Internet 选项”命令，在弹出的“Internet 选项”对话框中选择“内容”选项卡，然后单击“启用”按钮，弹出“内容审查程序”对话框。选择“常规”选项卡，单击“创建密码”按钮，弹出“创建监护人密码”对话框，在其中重新输入分级审查口令，单击“确定”按钮即可，如下图所示。

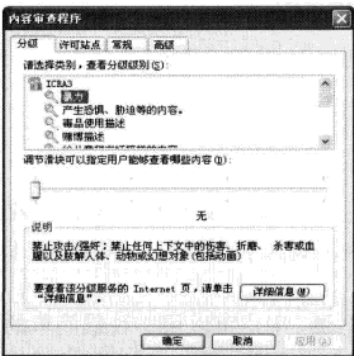


13.3.8 禁止 IE 访问某些站点

为了安全起见，有时需要限制 IE 访问某些站点，具体操作步骤如下：

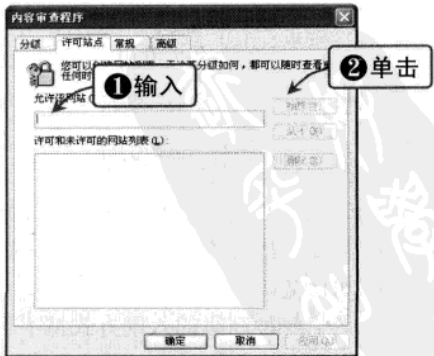
STEP 01 打开“内容审查程序”对话框

在 IE 窗口中依次单击“工具”|“Internet 选项”命令，在弹出的“Internet 选项”对话框中选择“内容”选项卡，单击“启用”按钮，弹出“内容审查程序”对话框，如下图所示。



STEP 02 “许可站点”选项卡

选择“许可站点”选项卡（如下图所示），在“允许该网站”文本框中输入禁止访问的站点地址，然后单击“从不”按钮，即可使输入的站点不能被访问；单击“始终”按钮，则将输入的站点列为始终都能访问的站点。





13.4 常见病毒和木马的防范技巧

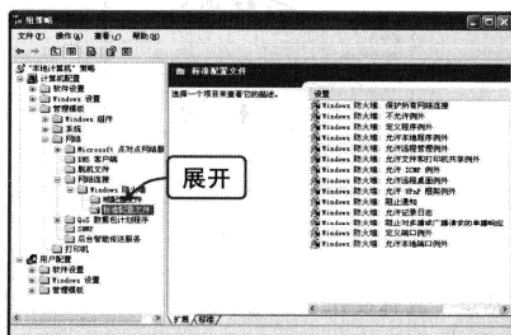
病毒和木马的侵害往往是造成计算机无法正常运行的主要原因，黑客经常利用病毒和木马对目标进行入侵。下面将介绍常见病毒和木马的防范技巧。

13.4.1 指定 Windows 防火墙阻止所有未经请求的传入消息

指定 Windows 防火墙阻止所有未经请求的传入消息的具体操作步骤如下：

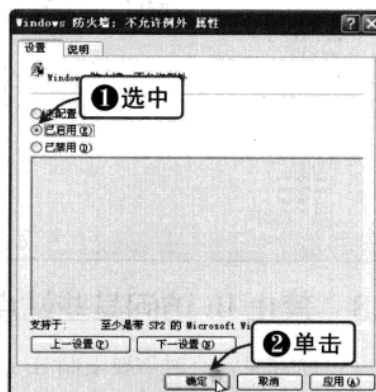
STEP 01 打开“组策略”窗口

在“组策略”窗口中依次展开“计算机配置”|“管理模板”|“网络”|“网络连接”|“Windows 防火墙”|“标准配置文件”选项，如下图所示。



STEP 02 打开 Windows 防火墙设置

双击右侧窗口中的“Windows 防火墙：不允许例外”选项，弹出“Windows 防火墙：不允许例外 属性”对话框，选中“已启用”单选按钮，并单击“确定”按钮即可，如下图所示。



13.4.2 处理感染病毒的计算机

如果一台电脑感染了病毒，就会成为病毒的工具和傀儡，发动对其他电脑的感染和攻击，这是病毒的特征之一。

在网络中为了防止已经感染病毒的电脑继续向其他电脑传播病毒，在发现病毒感染症状之后，应迅速采取措施将其隔离——除掉网线，然后启动杀毒软件彻底查杀病毒。对于无法在 Windows 下杀掉的病毒可以启动系统到 DOS 下，利用 DOS 版杀毒软件查杀。在 DOS 下由于病毒失去了对系统的依赖，就会很容易查杀干净。

13.4.3 定期检查敏感文件

任何杀毒和防火墙软件都不能完全确保系统不被入侵，黑客可以绕过重重防线侵入系统，特别是一些比较高级的黑客，它们进入系统后不声不响地潜伏下来，令用户根本感觉不到威胁的存在。

但无论何种高级的入侵方式都不可能不留下蛛丝马迹，用户可以用一种最简单的方法找到黑客程序，比如通过 Windows 搜索功能查找最近产生的程序文件。如果能够确认自己最

Chapter 13 黑客攻防实用技巧

近并没有安装任何程序，而在搜索后确实发现了一个最新的程序，那么很显然这就是一个黑客使用的程序。

因此，即使系统的补丁已经打得很齐全，病毒库也升级到最新版本，用户仍然需要警惕，定期对系统的一些敏感文件进行检查，保证及时发现那些未被杀毒软件发现的新型病毒和黑客程序。

13.4.4 识别隐藏的木马程序原文件

“隐藏”是木马的特性之一，每一种木马都有隐藏自己的技术，木马程序原文件隐藏就是其中的一种。

木马程序原文件隐藏有伪装文件名、伪装图标和伪装系统文件 3 种方式，下面进行简要介绍。

1. 伪装文件名称

由于在默认的情况下系统会隐藏自己的扩展名，所以木马程序就利用隐藏扩展名来达到伪装的目的，例如，木马的名称为 Filename.jpg.exe，木马程序本来为一个可执行文件，但在隐藏扩展名的情况下会显示为 JPG 图片文件。

2. 伪装图标

为了加强伪装文件名称的效果，木马程序的图标会换成相关的图片、文本等默认使用的图标。有的木马程序甚至利用空文件名再加透明图标来欺骗受害者。

3. 伪装成系统文件

木马的文件名称类似 Server、Explore 或 Iexploer，这类的文件放在系统文件夹里一般的用户很难辨别其真伪，有的木马程序做法更绝，会替换掉不常用的系统文件。

13.4.5 木马程序对通信端口的使用

木马程序使用了很多技术来隐蔽地使用通信端口，这些技术大体上可分为两类：寄生和潜伏。

1. 寄生

木马程序会寄生在已打开的服务通信端口上，如端口 80 等，平时只采用监听模式，收到正常的 HTTP 请求仍然把它交与 Web 服务器处理，只有当接收到特定信号时木马程序就会被启动，再重新打开一个新的通信端口。一般很少有人注意到平时所使用的通信端口，竟然会成为木马程序的宿主。所以在检查网络连接状态时，最好关闭不需要的程序，这样会减少打开的端口数量进而加快判断的速度。

2. 潜伏

木马程序的潜伏技术是利用监听 IGMP (Internet group managent protocol, 即互联网组管理协议)，再利用特别的 IGMP 信号来启动，由于 IGMP 无需使用通信端口，所以平时不会被通信端口扫描程序发现。使用 IGMP 激活技术的木马程序，平时很难被察觉，只有在它启动后打开通信端口才有可能被检测到。



13.4.6 木马程序隐藏运行进程的方法

在 Windows 9x 中，让木马图标不出现在任务栏中并非是一件难事，例如，在 VB 中，只要把 from 的 Visible 属性设置为 False，ShowInTaskBar 设为 False 程序就不会出现在任务栏里了。因此，很难发现木马的存在，为了检测木马程序用户必须得专门安装进程检查程序，如 DLLSpy。

但是，在 Windows 2000/Windows XP 操作系统中用户可以通过“任务管理器”轻易地查看到系统的进程，并且也能够很容易地结束进程。在这种情况下，木马的隐身术显然是失败的，更别说控制别人的计算机了。若让计算机管理员发现了这些非法的进程，便会马上中断其运行。为了克服这个问题，木马程序通常采用两种方式来解决隐藏或保护自身进程的问题。

1. 伪装成可信任进程

为了解决进程的问题，木马改装成类似于 Iexplore.exe、services.exe 等系统进程，使人难以看出与正常进程的差异。有时用户即使看出一些差异了，但由于对木马以及系统了解的比较少，也不敢轻易结束其进程。但对于一些心细的高手来说这样的木马就很难发挥作用了。

2. 不使用进程

在 DOS 和 Windows 下执行文件 exe 或 com 时，系统都会打开一个进程，那么有没有办法不使用进程呢？这就要靠 DLL（Dynamic Link Library，动态链接库）了，不使用进程的木马是采用把木马写成 DLL 文件的方式，这也就是所谓的 DLL 木马。要注意的是，DLL 文件是不能直接执行的文件，要运行写成 DLL 的木马程序有三种方法。

(1) 使用系统程序 Rundll32.exe 或是 Rundll.exe 调用 DLL

在 Windows 系统文件中有 Rundll32.exe 与 Rundll.exe 两个程序，这两个程序的功能是用来调用执行 DLL 中的函数，两者的区别是一个执行 32 位函数，另一个执行 16 位函数。具体的执行命令如下：

Rundll32.exe/Rundll.exe DllFileName FunctionName（命令格式是 rundll32.exe/Rundll.exe [DLL 名][函数][参数]）。

只要在启动中加入这样的一条命令，则系统启动后木马程序就会自动加载到内存。这时如果查看进程，根本就看不到与 DLLFileName 有关的进程，看到的只是 Rundll32.exe 进程，这是系统正常的进程，对于普通的用户相信没有人将这样的进程结束。

对付这种类型的木马，最好的办法就是检查 SYSTEM.INI、Win.INI、启动、服务等启动加载的项目，当发现使用 Rundll32.exe/Rundll.exe 的命令时稍加注意一下，木马程序就会被发现了。

(2) 使用反编译的陷阱技术

陷阱技术是一项比较高级的反编译技术，通常程序员经常使用这种技术。为了说明它的原理，下面来举一个例子。系统中有一个 DLL 文件 log.dll，首先将 log.dll 更名为 Oldlog.dll，然后将自己编写 DLL 命名为 log.dll 并复制到原 log.dll 所在的文件夹。在一般情况下，当系统调用 log.dll 时，已更新的 log.dll 会将调用转发给原系统 Oldlog.dll，但是若满足一定的条件替换的 log.dll 就会自己自动执行。利用这个原理，DLL 木马可以替换成任何一个常用的 DLL，当满足条件时就自动执行这个安全漏洞。幸好微软已经想到了，在 Windows 2000 与

免责声明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Windows XP 系统中 DLL 都使用了数字签名技术，通过它可以发现被保护的 DLL 文件是否被篡改；另外，在 system32 目录下有一个 dllcache 文件夹，这个文件夹中存放着大量的 DLL 文件（也包括一些重要的 exe 文件）。一旦发现 DLL 文件被篡改，它就会自动从 dllcache 中恢复这个文件。

虽然微软采取 DLL 保护措施,但是仍然有种种方法可以绕过 DLL 保护。例如先更改 dllcache 目录中的备份再修改 DLL 文件、或者利用 KnownDLLs 键值更改 DLL 的默认启动路径等,不过在可以预见的未来,微软必将更加小心地保护重要的 DLL 文件,采用此种技术的木马将会减少。

(3) 动态嵌入技术

DLL 木马的最高境界是动态嵌入技术，动态嵌入技术指的是将木马本身的代码嵌入正在运行的进程中的技术。理论上来说，在 Windows 中的每个进程都有自己的私有内存空间，别的进程是不允许对这个私有空间进行操作的，但实际上仍然可以利用种种方法进入并操作进程的私有内存。在多种动态嵌入技术中（钩子、挂接 API、远程线程），现在的大多数 DLL 木马都采用远程线程技术把自己挂在一个正常系统进程中，像 explorer.exe、svchost.exe、smss.exe 等无法结束的系统关键进程是 DLL 木马的最爱。

远程线程技术就是通过在另一个进程中创建远程线程 (Remote Thread) 的方法进入那个进程的内存地址空间。在 DLL 木马的范畴里, 这个技术也叫做“注入”, 当载体在那个被注入的进程里创建了远程线程并命令它加载 DLL 时, 木马就挂上去执行了, 这样没有新进程产生, 要想让木马停止唯有让挂接这个木马 DLL 的进程退出运行。但是由于载体大多是系统关键进程, 因此很多时候被感染者只能束手无策——它和 Explorer.exe 挂在一起了, 难道要关闭 Windows 吗?

由于 DLL 木马是挂着系统进程运行的，所以如果它本身写得不好，如没有防止运行错误的代码或者没有严格规范用户的输入，DLL 就会出错以致崩溃，而且 DLL 崩溃会导致它挂着的程序跟着遭殃，并且由于它挂接的是系统进程，因此导致的结局往往就是系统崩溃。

13.4.7 通过修改文件关联启动木马程序

修改文件关联是木马常用的启动手段，特别是国产木马，而国外的木马大都没有这个功能，比方说在正常情况下文本文件的打开方式为 Notepad.EXE 程序，但如果中了文件关联木马，则文本文件打开方式就会被修改为用木马程序打开，如著名的国产木马冰河就是属于这种情况。

“冰河”木马是将注册表中的 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值“C:\Windows\notepad.exe %1”改为“C:\Windows\SYSTEM\SYSEXPLR.EXE %1”，这样，当被植入木马的用户双击一个文本文件时，原本应用记事本程序打开的文件就将启动了木马程序。另外，不仅仅是 TXT 文件，其他诸如 HTM、EXE、ZIP、COM 等都可能是木马的目标，用户要多加小心。

13.4.8 防范木马的常用方法

随着网络的普及、硬件和软件的高速发展，网络安全显得日益重要。网络中比较流行的木马程序，传播速度比较快，影响比较严重，因此对于木马的防范就更加不能疏忽。



(1) 不要随意打开来历不明的邮件

现在许多木马都是通过邮件来传播的，当用户收到来历不明的邮件时请不要打开，应尽快删除。同时，要加强邮件监控系统，拒收垃圾邮件。

(2) 不要随意下载来历不明的软件

最好是在一些知名的网站下载软件，不要下载和运行那些来历不明的软件。在安装软件之前最好用杀毒软件查看是否含有病毒，然后才进行安装。

(3) 及时修补漏洞和关闭可疑的端口

一些木马都是通过漏洞在系统上打开端口留下后门，以便上传木马文件和执行代码，在把漏洞修补上的同时，需要对端口进行检查，把可疑的端口关闭。

(4) 尽量少用共享文件夹

如果必须共享文件夹，则最好设置账号和密码保护。Windows 系统默认情况下将目录设置成共享状态，这是非常危险的，最好取消默认共享。

(5) 运行实时监控程序

在网上时最好运行反木马实时监控程序和个人防火墙，并定时对系统进行病毒检查。

(6) 经常升级系统和更新病毒库

经常关注微软和杀毒软件厂商网站上的安全公告，这些网站通常都会及时地将漏洞、木马和更新公布出来，并在第一时间发布补丁和新的病毒库等。